DriveLock Administration

Dokumentation 2022.2

DriveLock SE 2022

Inhaltsverzeichnis

1 Hinweis zu dieser Dokumentation

Aufgrund der Überarbeitung und Umstrukturierung unserer gesamten Dokumentation finden Sie in diesem Dokument eine kurze Einführung in das DriveLock Operations Center (DOC), sowie Informationen zur Arbeit mit der DriveLock Management Konsole (DMC) und dem DriveLock Richtlinien Editor.

Im (alten) DriveLock Administrationshandbuch finden Sie noch Kapitel zu folgenden Themenbereichen: Laufwerks- und Gerätekontrolle, Netzwerkprofile und Informationen zum Einsatz von DriveLock mit Terminal Servern.

Außerdem bieten wir für verschiedene Themen eigenständige Dokumentationen an: Application Control, DriveLock Encryption (beinhaltet Disk Protection, File Protection, BitLocker Management, BitLocker To Go, Encryption 2-Go und DriveLock PBA), Defender Management, DOC Companion, DriveLock Events, Linux Agenten, macOS Agenten, Security Awareness, Self-Service Portal und Vulnerability Management.

Des weiteren gibt es ein Installationshandbuch und eine Endbenutzerdokumentation.

Die gesamte Produktdokumentation finden Sie auf DriveLock Online Help.

2 Mit DriveLock arbeiten

DriveLock ist eine moderne Security-Plattform, die Ihnen hilft, sich vor Cyberangriffen aller Art und dem Verlust wertvoller Daten zu schützen. Mit Managed Security Services bietet Ihnen DriveLock ein Hosting der kompletten DriveLock-Lösung in der Cloud an, verbunden mit Verwaltung durch unsere Sicherheitsexperten. Sie benötigen hierfür keine eigene Infrastruktur oder Software von Drittanbietern. Alternativ können Sie aber auch Ihre eigene Infrastruktur selber verwalten ('on-prem'). Wichtige Hinweise zu den Unterschieden finden Sie hier.

Dafür stellt Ihnen die Plattform eine Reihe von Sicherheitsfunktionen zur Verfügung, die Sie mit Hilfe folgender Konsolen verwalten können:

- DriveLock Operations Center (DOC)
- DriveLock Management Konsole (DMC)
- DriveLock Richtlinien-Editor

Hinweis: Beachten Sie, dass nicht alle Funktionalitäten gleichermaßen im DOC und in der DMC verfügbar sind.

3 DriveLock Operations Center (DOC)

Das DOC ist eine moderne browserbasierte Benutzeroberfläche für die DriveLock Zero Trust Platform. Mit dem DOC arbeiten können sowohl Kunden der DriveLock Managed Security Services, die unsere cloud-basierte Sicherheitslösung verwenden, als auch Kunden, die DriveLock 'on-premise' einsetzen und selbst verwalten. Einige Unterschiede bei der Verwendung sind hier erläutert.

Im DOC erhalten Sie eine Übersicht über den aktuellen Status aller Computer in Ihrem Unternehmen, die mit DriveLock verwaltet werden. Unterstützte Sprachen sind Deutsch und Englisch, der Sprachwechsel funktioniert mit einem Klick auf die jeweilige Sprache.

Sämtliche Funktionalitäten, die bisher im DriveLock Control Center (DCC) vorhanden waren, sind jetzt mit dem DOC möglich: Inventarisierung, Erstellung von Ereignis- und Statistikberichten, sowie forensischen Analysen, Durchführen von Wartungsaufgaben oder die Installation von DriveLock Agenten.

Mit Hilfe des DOC Companions kann auf den Richtlinien-Editor, der bis Version 2021.2 nur über die installierte DriveLock Management Konsole verfügbar war, zugegriffen werden. Dieser ermöglicht die Bearbeitung und Erstellung von Richtlinien, sowie Zugriff auf Einstellungen, die im DOC noch nicht verfügbar sind.

> Hinweis: Weitere Informationen finden Sie in der separaten **DriveLock DOC Companion** Dokumentation auf DriveLock Online Help.

3.1 Allgemeine Hinweise

DriveLock Managed Security Services und DriveLock 'On-Prem' verwenden eine fast identische DOC-Benutzeroberfläche.

Es gibt jedoch einige funktionale Unterschiede:

1. Anmeldeverfahren am DOC
   - Managed Services: Anmeldung über E-Mail-Aktivierung oder per SAML
   - On-Prem: Anmeldung als AD-Benutzer oder über Mitgliedschaft in einer AD-Gruppe

   > Hinweis: Der erste angemeldete Benutzer wird Administrator, alle weiteren werden Benutzer.

2. Deployment des DriveLock Agenten

- Managed Services: Herunterladen über WebInstaller / Agent
- On-Prem: Ausführen der Push-Installation

3. Konfiguration des DriveLock Agenten
   - Managed Services: Der Agent kann nicht remote konfiguriert werden
   - On-Prem: Der Agent kann konfiguriert werden (Mandant, Richtlinie usw.)

3.2 DriveLock Operations Center 'on-premise'

3.2.1 Anmeldung am DOC

Es gibt zwei Möglichkeiten, das DOC zu öffnen:

Über den **DriveLock Operations Center Weblink** im Startmenü wird die web-basierte Benutzeroberfläche des DOC gleich mit der richtigen URL in Ihrem Browser geöffnet. Sie können das DOC aber auch direkt aus Ihrem Browser öffnen, indem Sie im Browser manuell die URL **https://DES-SERVER:4568** eingeben.

Achtung: Das DOC kann nur in einer aktuellen Version von Google Chrome, Microsoft Edge, Mozilla Firefox oder Safari geöffnet werden. Ältere Webbrowser werden nicht unterstützt!

Hinweis: Beachten Sie bitte auch die Hinweise zur Verwendung von Zertifikaten für die einzelnen Browser.

3.2.2 Hinweise zur Verwendung von SSL-Zertifikaten

DriveLock verwendet für die Kommunikation mit dem DriveLock Operations Center (DOC) SSL-Zertifikate. Sie können diese bereits bei der Installation des DriveLock Enterprise Service (DES) angeben oder alternativ ein selbstsigniertes Zertifikat erstellen. Weitere Informationen zum Thema Zertifikate finden Sie im Installationshandbuch auf Drivelock Online Help.

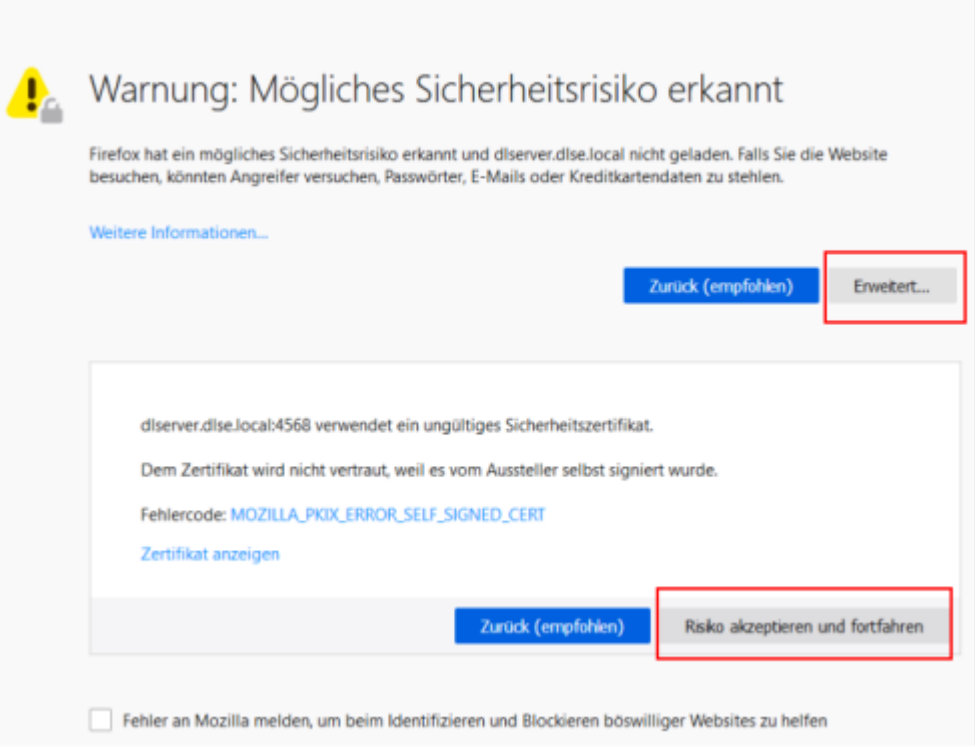
Hinweis: Wir empfehlen, sich ein Zertifikat für den DES von einer anerkannten Zertifizierungsstelle (CA) erstellen lassen!

Falls Sie ein selbstsigniertes Zertifikat verwenden, erscheinen beim Öffnen des DOC je nach Browser unterschiedliche Warnungen, weil das Zertifikat aus Sicht des Browsers nicht vertrauenswürdig ist.

In den Beispielen unten lautet der Name des DES dlserver.dlse.local.

Wenn Sie Mozilla Firefox verwenden, gilt folgendes:

Klicken Sie auf **Risiko akzeptieren und fortfahren**, um das Zertifikat zu akzeptieren. Sie müssen sich weder die Zertifikatsdetails anzeigen lassen, noch das Zertifikat importieren. Firefox fügt nur eine Sicherheitsausnahme für diese Webseite hinzu. Weitere Schritte sind nicht notwendig.

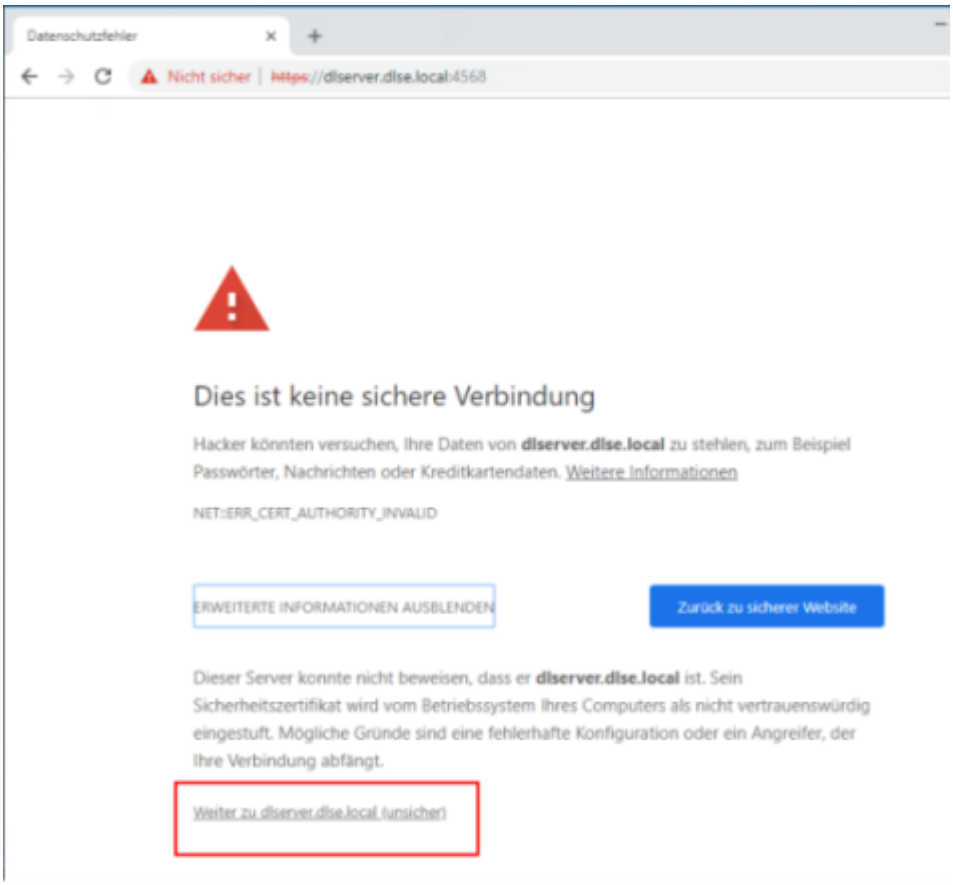


Für Google Chrome und Microsoft Edge gilt folgendes:

Bei beiden Browsern sollten Sie das Zertifikat in den Zertifikatsspeicher eintragen, damit Sie nicht bei jedem Start des DOC eine Warnung erhalten.

- Microsoft Edge:

- Google Chrome

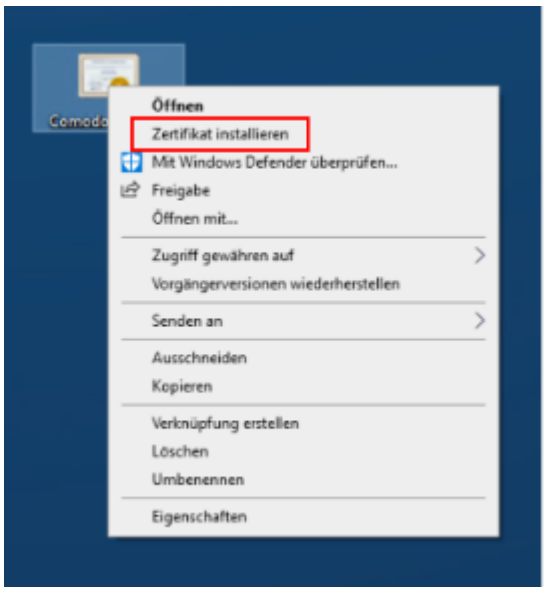


3.2.2.1 Zertifikate importieren

Gehen Sie folgendermaßen vor:

1. Akzeptieren Sie bei beiden Browsern die Warnung und öffnen Sie das Zertifikat.
2. Sie können sich die Details des Zertifikats ansehen und das Zertifikat mithilfe des Zertifikatimport-Assistents in den lokalen Zertifikatsspeicher importieren.

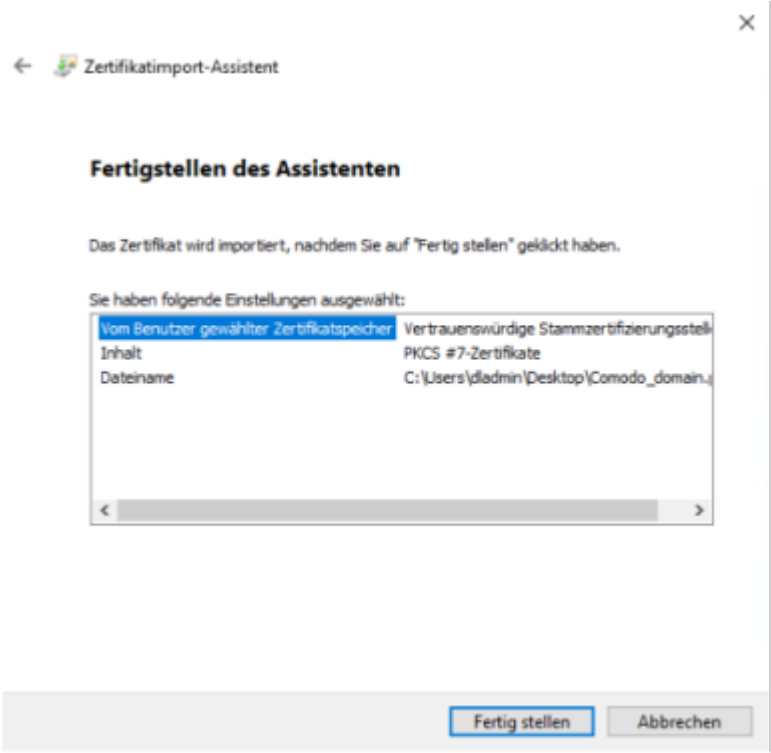
3. Speichern Sie das Zertifikat in einem Verzeichnis Ihrer Wahl.
4. Öffnen Sie das Kontextmenü des Zertifikats und klicken Sie auf **Zertifikat installieren**.



5. Der Zertifikatimport-Assistent öffnet sich. Lassen Sie auf der ersten Seite die Voreinstellung X.509.
6. Wählen Sie auf der nächsten Seite die Option Lokaler Computer aus.

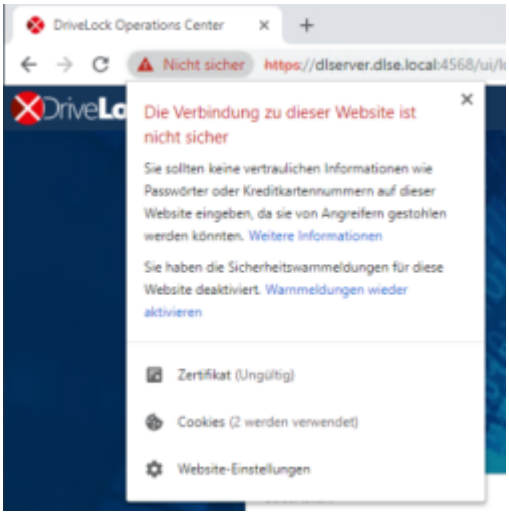
7. Auf der dritten Seite wählen Sie als Zertifikatsspeicher die Option **Vertrauenswürdige Stammzertifizierungsstelle**:

8. Klicken Sie im nächsten Dialog auf **Fertigstellen**.



9. Das Zertifikat ist nun eingetragen und beim nächsten Öffnen der DOC gelangen Sie ohne Fehlermeldung direkt zur Anmeldemaske.

Achtung: Beachten Sie jedoch, dass auch dann das Zertifikat vom Browser als nicht sicher angesehen wird und weiterhin folgende Warnung erscheint (im Beispiel unten bei Google Chrome):



3.3 Sicherheitseinstellungen im DOC

Der DriveLock Enterprise Service erzeugt pro Mandant ein eindeutiges Beitrittstoken (Join Token), das während der Installation eines Agenten angegeben werden muss, damit der Agent zu dem Mandanten hinzugefügt werden kann.

> Hinweis: Bestehende Agenten brauchen dieses Beitrittstoken nicht, die Prüfung findet nur bei Neuinstallationen statt.

Wenn der Agent aus dem DOC heraus installiert wird, wird das Beitrittstoken automatisch an das MSI übergeben.

Wenn man das DriveLock Agent Setup manuell ausführt, muss das Beitrittstoken als Parameter an das MSI übergeben werden:

`USEJOINTOKEN=1 JOINTOKEN=<Join Token>`, z.B.

```
msiexec /I "d:\DriveLock Agent X64.msi" /qb USESERVERCONFIG=1
CONFIGSERVER=https://dlserver.dlse.local:6067 USEJOINTOKEN=1
JOINTOKEN=c93a2959-0c10-444b-b700-6f8ec3630ad2
```

Ist das Token auf dem Agenten nicht vorhanden oder wird ein falsches angegeben, lässt sich zwar der DriveLock Agent installieren, wird aber vom DriveLock Enterprise Service abgewiesen. In diesem Fall kann das Join Token auch nachträglich mit dem Befehl `driveLock -SetJoinToken <Join Token>` gesetzt werden. Der DriveLock Service muss danach neu gestartet werden oder der Befehl `driveLock -updateconfig` aufgerufen werden.

Sollte die Registrierung fehlschlagen, wird auf dem Agenten eine Fehlermeldung im Tray Icon angezeigt. Der DriveLock Enterprise Service generiert ein entsprechendes Event mit dem Grund für das Ablehnen des Agenten.

ID	Type	Bedeutung
2105	Success audit	An agent successfully registered
2106	Failure audit	The agent tried to register with the invalid join token '%1'
2107	Failure audit	The agent tried to update its agent ID to the new value '%1'. This is not permitted. Please reset the agent registration via

		DOC if this change is intended
2108	Failure audit	Rejected access to DES for agent. The agent sent the not existing agent ID '%1'
2109	Failure audit	Rejected access to DES for agent. The agent sent the agent ID '%1' which does not belong to it. The conflicting data (name/ID) is: %2

3.3.1 Sicheres Hinzufügen neuer Agenten

In der Ansicht **Installation** im Menü **Konfiguration** im DOC können Sie auf dem Reiter **Sicherheitseinstellungen** angeben, dass ein DriveLock Agent einem Mandanten nur dann hinzugefügt werden darf, wenn er über einen Beitrittstoken (Join ID) verfügt.

Die Option **Agenten müssen ein Beitrittstoken vorweisen, damit sie in die Liste der verwalteten Computer aufgenommen werden** ist pro Mandant aktivierbar bzw. deaktivierbar. Als Standardeinstellung ist die Option deaktiviert.

Der DriveLock Enterprise Service (DES) kann jeden einzelnen Agenten identifizieren und somit sicherstellen, dass die Daten, die von einem Agenten kommen, auch tatsächlich von ihm und nicht einem anderen Computer geschickt wurden. Damit diese Prüfung stattfindet, muss im DOC die Sicherheitseinstellung **Agentenidentität verifizieren** aktiviert werden.

> Hinweis: Alle DriveLock Agenten müssen mindestens die Version 2021.2 haben, damit sich diese Einstellung aktivieren lässt. Sollten noch ältere Agenten existieren, bleibt die Einstellung ausgegraut und eine Liste der noch nicht aktualisierten Computer kann angeschaut werden.

Die Agentenidentität kann auch zurückgesetzt werden, indem Sie im Kontextmenüs eines verwalteten Computers den Menübefehl **Erweitert** auswählen und dann auf **Agentenidentität zurücksetzen** klicken. Dies kann im Zusammenhang mit der Neuinstallation eines Golden Images erforderlich sein.

3.3.1.1 Szenarien für die Verwendung von Beitrittstoken

- **Einen existierenden Computer neu installieren**

  Der Computer wird komplett neu installiert. Das Computer-Objekt im DriveLock Enterprise Service (DES) existiert jedoch bereits. Der DriveLock Agent wird nach der Betriebssysteminstallation unter Angabe des Beitrittstokens installiert. In diesem Fall muss das Beitrittstoken im DOC manuell zurückgesetzt werden. Das kann im

Kontextmenü des Computers erfolgen. Wenn dies nicht erfolgt, schlagen sämtliche SOAP Calls des Agenten fehl, weil durch die neue Installation des MSI ein neues Beitrittstoken generiert wird, das aber nicht registriert werden kann, da ja bereits ein Beitrittstoken bekannt ist. Auf dem Agenten wird nun eine Fehlermeldung angezeigt, dass die Verbindung zum DES nicht möglich ist.

- **Agent neu installieren**

  Wenn nur der DriveLock Agent neu installiert wird, ohne dass die DriveLock Einträge aus der Registry gelöscht werden, muss nichts beachtet werden. Sollten die Registry-Einträge ebenfalls gelöscht worden sein, ist der Ablauf identisch zum oben beschriebenen Punkt "Einen existierenden Computer neu installieren".

- **Computer umbenennen**

  In diesem Fall ist auch nichts zu beachten, da der DriveLock Agent erkennt, dass der Computer umbenannt wurde und teilt das dem DriveLock Enterprise Service mit. Es kann sein, dass der DriveLock Service kurzfristig die Kommunikation mit dem Agenten verweigert, bis die Umbenennung des Computers bekannt wird.

- **Agent aktualisieren von älterer Version**

  Auch hier gibt es nichts zu beachten. Ein Beitrittstoken wird nicht benötigt, da das Computer-Objekt schon existiert.

3.3.2 DriveLock in Virtualisierungsumgebungen

Wenn Sie in Ihrem Unternehmen eine VDI (Virtual Disk Image) Umgebung haben oder mit Festplatten-Images arbeiten, in denen ein DriveLock Agent vorinstalliert wird, müssen die Klon-Abbilder (auch als Golden Images bezeichnet) als solche dem DriveLock Enterprise Service (DES) bekannt gemacht werden.

Gehen Sie folgendermaßen vor:

Öffnen Sie im DOC die Ansicht **Computer** . Wählen Sie dort Ihr Golden Image aus und öffnen Sie die Konfiguration dieses Computers.

Aktivieren Sie die Einstellung **Computer wird als Image für andere Computer verwendet**. Damit erkennt DriveLock die Computer, die immer wieder unter dem gleichen Namen neu erzeugt werden, und die gesamte Historie bleibt erhalten.

In der Computerübersicht können Sie die Spalten **Image für andere Computer** sowie **Erstellt aus** einblenden, um eine Übersicht zu bekommen, welche Klon-Abbilder es gibt und welche Computer daraus erzeugt wurden.

Hinweis: Wenn Sie ein Golden Image komplett neu installieren müssen und die Option **Agentenidentität verifizieren** in den Sicherheitseinstellungen im DOC aktiviert ist, müssen Sie die Agentenidentität dieses Computers zunächst im DOC zurücksetzen. Dies ist wichtig, damit sich die geklonten Images beim ersten Start mit dem DES verbinden können.

3.4 Azure AD-Integration

Unternehmen, die ihre Infrastruktur und Benutzer-Berechtigungen zentral über die Cloud-Plattform Microsoft Azure und Azure Active-Directory verwalten, können die dort vorhandenen Gruppen in DriveLock synchronisieren und für Zugriffsberechtigungen und die Zuweisung von DriveLock Sicherheitsrichtlinien auf die gleiche Art und Weise verwenden, wie das bisher schon mit einem lokalen Active-Directory möglich war.

Computergruppen aus dem AAD werden in DriveLock wie statische Gruppen behandelt, mit dem Unterschied, dass sie automatisch durch eine Synchronisation gepflegt werden und nicht manuell durch den Benutzer.

Durch die Integration können Sie folgende Ziele erreichen:

1. **Zuweisen von Richtlinien auf Computergruppen**

   Computergruppen, die mit einem AAD verbunden sind, dienen als Ziel von Richtlinienzuweisungen.
   Sie stehen innerhalb von DriveLock als statische Computergruppen zur Verfügung. Diese Gruppen müssen für DOC und DriveLock Management Konsole (DMC) lesbar sein.

2. **Verwenden von Computergruppen in Richtlinien**

   Innerhalb von Richtlinien können Sie AAD-Gruppen analog zu statischen Gruppen verwenden. Regeln für einzelne Computer müssen über den Computernamen erstellt werden.

3. **Verwenden von Benutzern und Benutzergruppen in Richtlinien**

   Für Benutzer wird nicht die SID wie bisher verwendet, sondern der AAD-Kontoname. Dies ist eine Adresse z.B. in der Form "user@mydomain.onmicrosoft.com".
   AAD-Benutzergruppen sind auch innerhalb der DMC als DriveLock Benutzergruppe auswählbar. Die zur Verfügung stehenden Benutzergruppen und ihre Mitglieder werden analog zu den Computergruppen über einen Synchronisationsmechanismus eingepflegt.

4. **Anmelden auf Basis von Rollen und Berechtigungen über Azure AD Benutzer-Gruppen**

   Bei der Rollenzuweisung können Sie eine AAD-Benutzergruppe zu wählen. Wenn sich ein Benutzer am DOC über SAML anmeldet, ermittelt der DES die AAD-Benutzergruppen, in denen der Benutzer Mitglied ist. Die weitere Logik unterscheidet sich nicht mehr vom normalen AD.

5. **SB-Freigabe**

   Azure AD-Benutzer- und Computergruppen können in der SB-Freigabe verwendet werden

3.4.1 Einstellungen für Azure AD

Durch die Integration von Azure AD werden Gruppen und deren Mitglieder von Azure AD nach DriveLock synchronisiert. Damit dies funktioniert, müssen Sie zuerst einige Konfigurationsschritte in Azure AD durchführen und dann die dadurch erzeugten Daten in den entsprechenden Textfeldern im DriveLock Operations Center (DOC) einfügen.

1. **Einstellungen unter "Overview"**

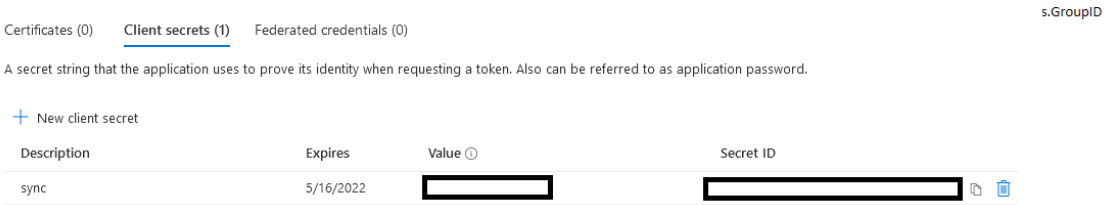
   Für die Synchronisation sind folgende Daten aus der Azure AD-Übersicht notwendig: Mandanten-ID ("Tenant ID") und primäre Domäne ("Primary domain").

2. **Applikation registrieren und konfigurieren**

   Erstellen Sie eine neue Applikation im Abschnitt "App registrations" und notieren Sie die "Application ID (Client ID)" aus der Übersichtsseite.

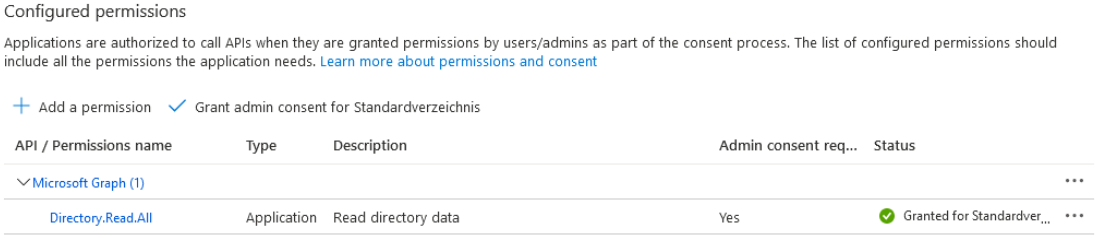
   - **Geheimen Schlüssel erzeugen**

     Erzeugen Sie einen neuen geheimen Schlüssel ("Client secret") im Abschnitt Zertifikate und geheime Schlüssel ("Certificates & secrets"). Sie benötigen den kompletten Inhalt aus der Spalte "Value".



- **Berechtigungen setzen**

  Vergeben Sie im Abschnitt "API permissions" die Rechte wie in der Abbildung zu sehen:



SAML Konfiguration

Sie können optional eine SAML-Konfiguration mit der Azure AD-Konfiguration verknüpfen. Dies ermöglicht die Anmeldung mit Azure AD-Benutzern denen Rechte über die Zugehörigkeit in einer Azure AD-Gruppe zugewiesen wurde.

3.5 Gruppen

3.5.1 DriveLock-Gruppen erstellen

Es gibt zwei verschiedene DriveLock-Gruppen:

Statische Computergruppen werden definiert durch manuelles Hinzufügen von Computern, Gruppen oder Organisationseinheiten aus dem Active Directory (AD), aus einzelnen Computern (die individuell nach Namen hinzugefügt werden) oder aus bereits bestehenden DriveLock-Gruppen (auch Azure AD-Gruppen).

Dynamische Computergruppen werden aus den Ergebnissen von Abfragen (Filterkriterien) definiert, wie z.B. Abfrage nach Betriebssystemversion, IP-Bereich, Windows-Version uva. mehr. Die Gruppenzugehörigkeit eines DriveLock Agenten wird dabei folgendermaßen ermittelt: Zunächst werden die Filterkriterien in einer Datenbank gespeichert. Die Kriterien werden an die Agenten-Computer übermittelt, dort ausgewertet und anschließend erfolgt eine Rückmeldung über die jeweilige Gruppenzugehörigkeit. Nach Aktualisierung der Konfiguration werden die einzelnen Mitglieder in den Eigenschaften der dynamischen Gruppe (Reiter Aktuelle Mitglieder) angezeigt.

DriveLock-Gruppen lassen sich im **DriveLock Operations Center** im Menü **Konfiguration** in der Ansicht **Gruppen** erstellen. Über das Symbol **+** können Sie entweder statische und dynamische DriveLock-Gruppen hinzufügen. Sie können auch eine Kopie einer bereits vorhandenen Gruppe erstellen.

Azure AD-Gruppen werden nach DriveLock synchronisiert, indem die Azure AD-Integration angestoßen wird. Welche Einstellungen Sie hierfür vornehmen müssen, lesen Sie hier.

3.5.2 Statische Computergruppe

Um eine statische Computergruppe zu erstellen, gehen Sie folgendermaßen vor:

1. Klicken Sie auf **+ Gruppe hinzufügen** und wählen Sie **Statische Gruppe erstellen**.
2. Geben Sie einen Namen für die Gruppe an und fügen ggf. eine Beschreibung hinzu.
3. Ihre Gruppe erscheint in der Liste. Klicken Sie auf den Namen, um die Gruppe zu bearbeiten.
4. Unter **Definitionen** haben Sie nun die Möglichkeit, statische Gruppenmitglieder hinzuzufügen. Klicken Sie **+ Gruppenmitglied hinzufügen**.
   Hier haben Sie folgende Auswahlmöglichkeiten:
   - AD Computer / AD-Gruppe: Wählen Sie einzelne Computer oder Gruppen direkt aus dem AD aus und fügen diese Ihrer statischen Gruppe hinzu.
   - OU-Container: Wählen Sie die Computer aus einer AD Organisationseinheit (OU) aus.
   - Computername: Fügen Sie einzelne Computer nach Namen der Gruppe hinzu.
   - DriveLock-Gruppe: Sie können auch eine vorher erstellte DriveLock-Gruppe (dynamisch oder statisch) hinzufügen.
   - Azure AD-Gruppe: Wenn Sie bereits Azure AD-Gruppen in DriveLock integriert haben, können Sie diese hier ebenfalls auswählen.

   Hinweis: Beachten Sie bitte, dass Platzhalter bei statischen Gruppendefinitionen nicht verwendet werden können.

5. Nachdem Sie die Konfiguration aktualisiert haben, erscheinen jetzt auf der Registerkarte **Aktuelle Mitglieder** eine Liste der Computer, die Ihrer statischen Gruppe angehören. Im Beispiel sind das die Computer DLCLIENT01 und DLCLIENT04. In der Spalte **Ermittelt durch** sehen Sie, auf welchem Weg die Gruppenmitgliedschaft ermittelt wurde. Wenn Gruppen über die DriveLock Management Konsole hinzugefügt

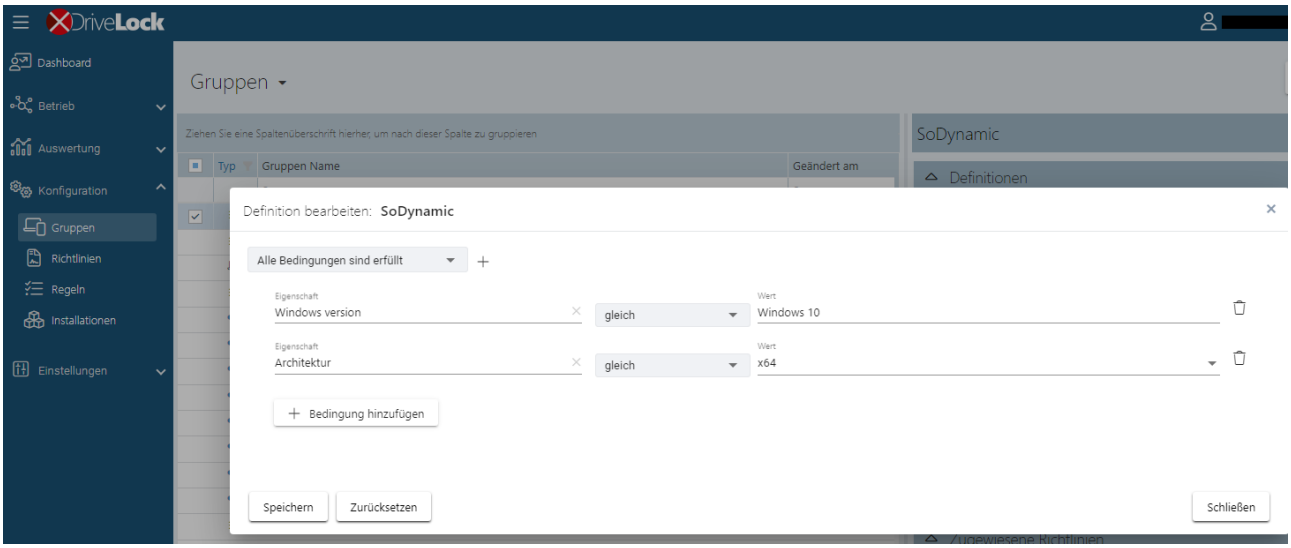
werden, wird Server als Ermittlungsquelle angegeben.
Sobald der Client seine Gruppenmitgliedschaft an den DES zurückgemeldet hat, wird Client als Ermittlungsquelle angegeben.

Im Kapitel Verwendung von Gruppen in Richtlinien finden Sie Erläuterungen zu den Reitern **Richtlinien** und **Zuweisungen**.

3.5.3 Dynamische Computergruppe

Um eine dynamische Computergruppe zu erstellen, gehen Sie folgendermaßen vor:

1. Klicken Sie auf **+ Gruppe hinzufügen** und wählen Sie **Dynamische Gruppe erstellen**.
2. Geben Sie einen Namen für die Gruppe an und fügen ggf. eine Beschreibung hinzu.
3. Der Dialog **Definition bearbeiten** wird geöffnet. Hier wählen Sie die Filterkriterien aus, die für Ihre Gruppe gelten sollen. Sie können z.B. die Windows-Version (Windows 10 als Wert) auswählen und danach die Architektur. Als Operator ist in diesem Beispiel 'gleich' gewählt worden. In anderen Fällen können Sie jedoch aus einer Liste von verschiedenen Operatoren auswählen.



Jetzt können Sie die erstellte dynamische Gruppe in der Konfiguration und Zuweisung von Richtlinien verwenden.

3.5.3.1 Filterkriterien für dynamische Gruppen (DOC)

Im folgenden finden Sie eine Erläuterung der Filterkriterien (Eigenschaften), die Sie für die Definition von dynamischen Gruppen verwenden können.

Filterkriterium	Verfügbar ab DriveLock Version	Typ	Wert, Name, Beispiel
AD-Computereigenschaften	2022.1	unbekannt, Integer	Die möglichen Attribute bzw. Werte sind im Attribute Editor im Domänen Controller unter Active Directory-Benutzer und -Gruppen zu finden Alle Computer aus einer bestimmten Abteilung (Attribut Department aus dem AD)
Architektur	2019.1	Enum	x86, x64
Betriebssystem-Build	2022.1	String	21H2
Betriebssystemname	2019.1	String	Windows 10 Pro
Betriebssystemtyp	2019.2	Enum	mögliche Betriebssysteme (Linux, Windows)
BIOS-Hersteller	2022.1	String	
BIOS-Version	2022.1	String	
BIOS-Zeitstempel	2022.1	Datum / Zeit	

Filterkriterium	Verfügbar ab DriveLock Version	Typ	Wert, Name, Beispiel
Computername	2019.1	String	
Defender Service-Version	2022.1	String	
Defender-Status	2022.1	Enum	Aktiv, Inaktiv, Teilweise aktiv
Distinguished Name	2022.1	String	CN=PC01,CN=Computers,DC=DLSE,DC=local
Domänenname	2022.1	String	
DriveLock-Version	2019.1	Version	
IP4-Bereich	2019.1	IP-Adressliste	Die entsprechenden IP4-Bereiche müssen eingegeben werden
Ist Server	2019.1	Bool	Ja, Nein
Ist Testumgebung	2019.1	Bool	Ja, Nein
Offene Schwachstelle	2022.1	Stringliste	Bezeichnung der Schwachstelle muss eingegeben werden

Filterkriterium	Verfügbar ab DriveLock Version	Typ	Wert, Name, Beispiel
Registry	2019.1	unbekannt, Integer	Registry-Schlüssel und Name muss herausgesucht und angegeben werden
SMBIOS-Version	2022.1	String	
TPM-Version	2022.1	Version	
TPM vorhanden	2022.1	Bool	Ja, Nein
Windows-Version	2019.1	Version	

Beispiele für die Verwendung der Operatoren in Kombination mit dem entsprechenden Typ:

Operator	Typ	Beispiel
gleich / ungleich	alle Typen außer Listen	Architektur gleich x64
entspricht	Strings (Platzhalter möglich)	Computername entspricht PC*
größer / größer gleich / kleiner / kleiner gleich	Integer, Versionen	DriveLock Version größer 21.2.5
beinhaltet Wert	nur für Listen	Offene Schwachstelle beinhaltet Wert CVE-2022-123

Operator	Typ	Beispiel
beinhaltet Bereich	IP-Adresslisten, Datumsangaben	IP-Bereich beinhaltet Bereich 192.168.0.0 bis 192.168.255.255

3.5.4 Verwendung von Gruppen in Richtlinien

Verwendet werden können statische und dynamische Gruppen in sämtlichen Whitelist-Regeln (Laufwerks- und Geräte-Whitelist-Regeln), Anwendungsregeln, Dateifilter-Vorlagen und Konfigurationsfiltern. Ebenso können Sie beide Gruppen für die Definition von Regeln für Security Awareness verwenden.

Hinweis: Statische und dynamische DriveLock-Gruppen müssen zuerst definiert werden, bevor sie in Richtlinien verwendet werden können. Es gibt keine vordefinierten DriveLock-Gruppen, die sofort einsetzbar sind.

Nach der Definition der DriveLock-Gruppe wird bei den Gruppeneigenschaften unter dem Menü **In Richtlinien verwendet** die jeweilige Verwendung angezeigt.

Achtung: Bitte beachten Sie, dass eine Anbindung an einen DES zwingend notwendig ist, um das Gruppenprinzip umsetzen zu können. Clients, die nur zeitweise keine Verbindung zum DES haben, werden bei der nächsten Verbindung mit den aktuellen Richtlinien (und Gruppeneinstellungen) wieder auf den neuesten Stand gebracht.

3.6 Laufwerks- und Anwendungsregeln im DOC

Um schnelle Freigaben zu ermöglichen, können Laufwerks- und Anwendungsregeln aus folgenden Ansichten im DOC erstellt werden:

Laufwerksregeln

1. Im Menü **Auswertung** in der Ansicht **Ereignisse**:
   Ereignisse, die Laufwerksdaten liefern, können als Quelle für eine Laufwerksregel verwendet werden. Über die Option **Laufwerksereignisse** in der vertikalen Aufteilung des Fensters können Sie sich die entsprechenden Ereignisse anzeigen lassen. Die dazugehörigen Laufwerke sind unter **Zugehörige Objekte** dargestellt. Klicken Sie hier auf **Laufwerke**, und öffnen danach das Kontextmenü des Laufwerks. Über den Menüpunkt **Zu Regel hinzufügen** wird das Laufwerk einer bestehenden Regel hinzugefügt.

Über den Menüpunkt **Regel erstellen** können Sie eine neue Regel erstellen, in der die Daten des jeweiligen Laufwerks bereits eingetragen sind.

2. Im Menü **Auswertung** in der Ansicht **Inventar** unter **Laufwerke**:
   Auf diesem Reiter sind alle Laufwerke mit den zugehörigen Informationen aufgelistet. Die Detailansicht zeigt eine Liste aller Richtlinien und Regeln, die bereits für das ausgewählte Laufwerk gelten. Auch hier können Sie über die entsprechenden Menüpunkte Laufwerke zu einer bestehenden Regel hinzufügen bzw. eine neue Regel erstellen.
3. Im Menü **Konfiguration** in der Ansicht **Regeln** sind alle bereits erstellten Laufwerksregeln aufgelistet. Hier können Sie über die Schaltfläche **Laufwerks-Regel erstellen** eine neue Regel erstellen. Bei dieser Option müssen Sie alle Daten manuell eintragen.

Anwendungsregeln

Für die Erstellung von Anwendungsregeln muss Application Control lizenziert sein und folgende Ereignisse müssen konfiguriert sein, damit der DriveLock Agent diese zum DES senden kann.

- 473: Prozess gesperrt
- 474: Prozess gestartet
- 648: DLL gesperrt
- 649: DLL geladen

1. Im Menü **Auswertung** in der Ansicht **Ereignisse**:
   Ereignisse, die Daten über Anwendungen liefern, können als Quelle für eine Anwendungsregel verwendet werden. Über die Option **Application Control** in der vertikalen Aufteilung des Fensters können Sie sich die Ereignisse für die Applikationskontrolle anzeigen lassen. Wählen Sie ein entsprechendes Ereignis aus und klicken Sie den Menüpunkt **Anwendungsregel erstellen**. Sie können so eine neue Regel erstellen, in der die Daten der Anwendung (Pfad, Hash, Version usw.) bereits eingetragen sind. Beachten Sie bitte, dass Sie mindestens eine der angezeigten Dateieigenschaften auswählen.
2. Im Menü **Auswertung** in der Ansicht **Inventar** unter Installierte Software oder Ausführbare Dateien:
   Hier sind Prozesse aufgelistet, die in Anwendungsregeln verwendet werden können.

3. Im Menü **Konfiguration** in der Ansicht **Regeln** sind alle bereits erstellten Anwendungsregeln aufgelistet. Hier können Sie über die Schaltfläche **Anwendungsregel erstellen** eine neue Regel erstellen. Bei dieser Option müssen Sie alle Daten manuell eingeben.

Hinweis: Weitere Informationen zu Anwendungsregeln, insbesondere zur Datei-Eigenschaften-Regel, finden Sie in der separaten Application Control Dokumentation auf DriveLock Online Help.

3.6.1 Regeln für Laufwerke erstellen

Gehen Sie folgendermaßen vor:

1. Nachdem Sie die Option **Regel erstellen** ausgewählt haben, öffnet sich ein Assistent.
2. Auf dem Reiter **Eigenschaften** geben Sie als einen Regelnamen ein und wählen den Regeltyp aus. Dieser bestimmt das Grundverhalten der Regel:
   - **Für bestimmte Benutzer oder Computer erlauben**: Dies gibt die Laufwerke für ausgewählte Benutzer an ausgewählten Computern frei.
   - **Für alle erlauben**: Dies gibt die Laufwerke für alle Benutzer an allen Computern frei.
   - **Für alle verbieten**: Dies sperrt die Laufwerke für alle Benutzer an allen Computern.
3. Die Laufwerke für die neue Regel werden auf dem Reiter **Liste der Laufwerke** aufgelistet. Falls es bereits Regeln für die Laufwerke gibt, wird eine Warnung angezeigt. Falls nur ein Laufwerk der Regel hinzugefügt wird, ist es möglich die Merkmale des Laufwerks zu editieren und ein Kommentar zu vergeben. Bei den Laufwerksmerkmalen werden Wildcards (*, ?) unterstützt, es ist also möglich z.B. einen Bereich von Seriennummern einzuschränken.
4. Auf dem Reiter **Berechtigungen** können Benutzer und Gruppen aus dem AD Inventar ausgewählt und der Regel hinzugefügt werden. Berechtigungen für Lesen, Schreiben und Ausführen können hier ebenfalls konfiguriert werden. Bei der Computerauswahl können Computer und Gruppen aus dem AD Inventar und DriveLock Gruppen hinzugefügt werden.
5. In den Optionen der Regel können folgende zusätzliche Konfigurationen vorgenommen werden:
   - **Benutzer muss Verwendungsrichtlinie akzeptieren**: Der Zugriffe auf ein Laufwerk darf erst dann erfolgen, wenn der Anwender das Lesen einer

Verwendungsrichtlinie bestätigt.

- **Verschlüsselung erzwingen**
- **Unverschlüsselte Laufwerke automatisch verschlüsseln**

> Hinweis: Bitte beachten sie, dass für erzwungene Verschlüsselung die Konfiguration der Verschlüsselung und Wiederherstellung in einer anderen Richtlinie konfiguriert werden muss. Weitere Informationen zur Verschlüsselung finden Sie in der Encryption Dokumentation auf DriveLock Online Help.

3.6.2 Regeln für Anwendungen erstellen

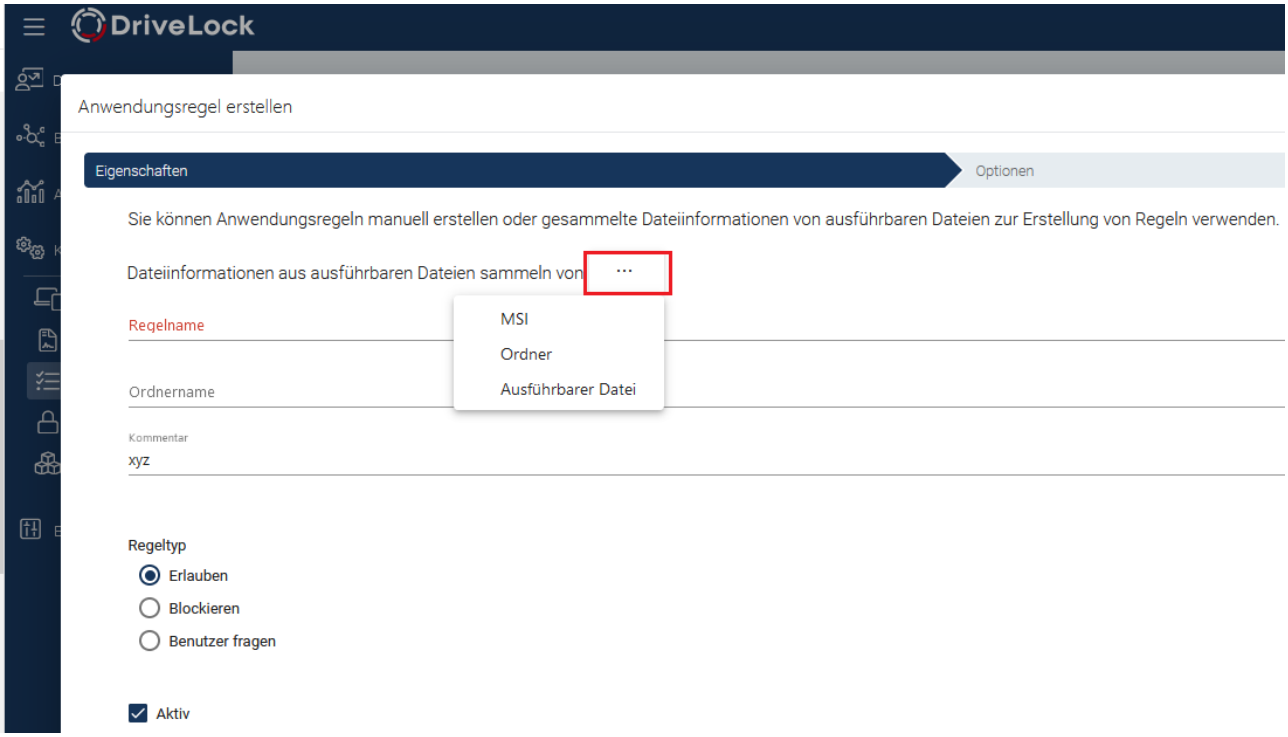
> Hinweis: Weitere Informationen zu Anwendungsregeln finden Sie in der separaten Application Control Dokumentation auf DriveLock Online Help.

Um eine Anwendungsregel im DOC zu erstellen, gehen Sie folgendermaßen vor:

1. Nachdem Sie die Option **Anwendungsregel erstellen** ausgewählt haben, öffnet sich ein Assistent.
2. Auf dem Reiter **Eigenschaften** entscheiden Sie zunächst, ob Sie eine Anwendungsregel manuell erstellen wollen oder ob Sie für die Erstellung Dateiinformationen von ausführbaren Dateien verwenden wollen.
   Bei der manuellen Erstellung geben Sie einen Regelnamen ein und wählen den Regeltyp aus. Dieser bestimmt das Grundverhalten der Regel:
   - **Nicht blockieren**: Diese Einstellung entspricht dem Regeltyp Whitelist, die ausgewählte Anwendung ist erlaubt und darf ausgeführt werden.
   - **Blockieren**: Diese Einstellung entspricht dem Regeltyp Blacklist, die ausgewählte Anwendung ist verboten und darf nicht ausgeführt werden.
   - **Benutzer fragen**: Mit diesem Regeltyp wird eine Anwendung zwar erlaubt (Whitelist), aber der Benutzer muss den Start bestätigen.
   - **Aktiv**: Diese Option ist standardmäßig gesetzt. Wenn Sie die Regel erstellen, aber nicht gleich aktivieren wollen, können Sie das Häkchen entfernen.
3. Auf dem Reiter **Optionen** geben Sie an, anhand welcher Kriterien (Dateieigenschaften) eine Anwendung erlaubt oder blockiert werden soll.

3.6.2.1 Dateiinformationen von ausführbaren Dateien verwenden

Über die Optionen **MSI**, **Ordner** oder **Ausführbare Datei** besteht die Möglichkeit, sich mehrere Anwendungsregeln gleichzeitig erstellen zu lassen.



Wenn Sie beispielsweise eine MSI auswählen, entpackt DriveLock im Hintergrund die gewählte MSI und erstellt daraufhin Vorschläge für Regeln mit den entsprechenden Regelkriterien. Innerhalb der Regeln wird eine Standardauswahl der gefundenen Kriterien (Informationen) gruppiert.

Sie können die Vorschläge annehmen oder ablehnen (indem Sie die Häkchen in den Checkboxen entfernen) und nur die Kriterien verwenden, die Ihnen sinnvoll erscheinen.

> Hinweis: Bitte bedenken Sie immer den Sicherheitsaspekt bei der Auswahl Ihrer Kriterien.

Die Regeln werden dann gruppiert und unter dem angegebenen Namen gespeichert und unter Anwendungsregeln angezeigt. Hier können Sie die einzelnen Regeln bearbeiten, aktivieren, deaktivieren oder löschen.

> Hinweis: Weitere Informationen zu Anwendungsregeln finden Sie in der Application Control Dokumentation auf DriveLock Online Help.

3.6.2.2 Anwendungsregeln über ausführbare Dateien erstellen

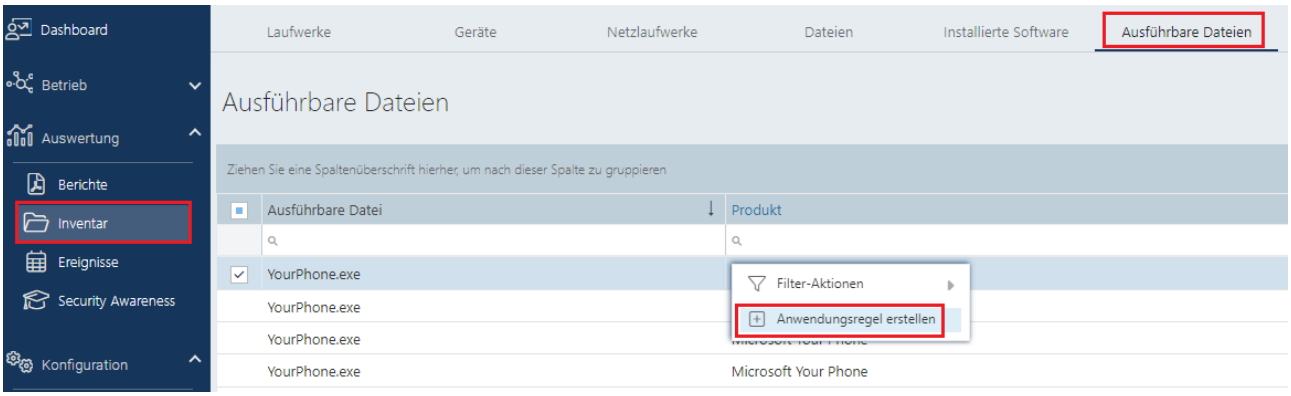
In der Liste erscheinen nur die ausführbaren Dateien, zu denen der DriveLock Agent Ereignisse gesendet hat und die bereits in der Anwendungshashdatenbank hinterlegt sind.

Um für einzelne oder mehrere ausführbare Dateien eine Regel zu erstellen, gehen Sie folgendermaßen vor:

Wählen Sie die gewünschte(n) Dateie(n) aus, öffnen Sie das Kontextmenü und dann die Option **Anwendungsregel erstellen**. Der Regelerstellungsassistent öffnet sich und erstellt automatisch Regeln mit den passenden **Eigenschaften**.

Auf dem Reiter **Optionen** sind die Regelkriterien aufgelistet.

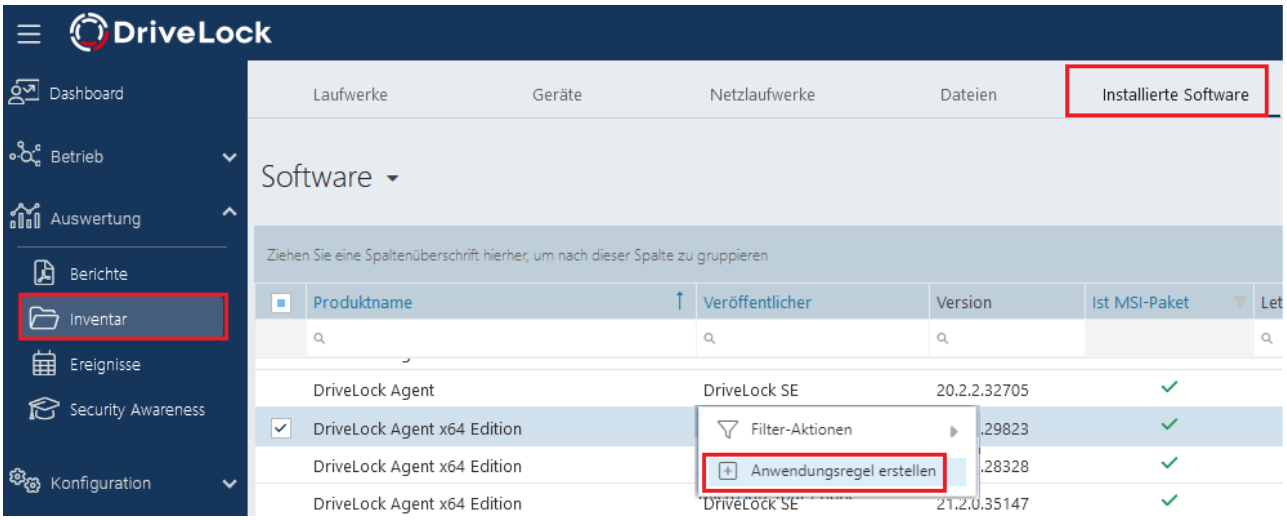
Auf dem Reiter **Überprüfen** können Sie Ihre Regeleinstellungen nochmals überprüfen, bevor Sie dann auf **Fertigstellen** klicken, um die Regeln zu erstellen.

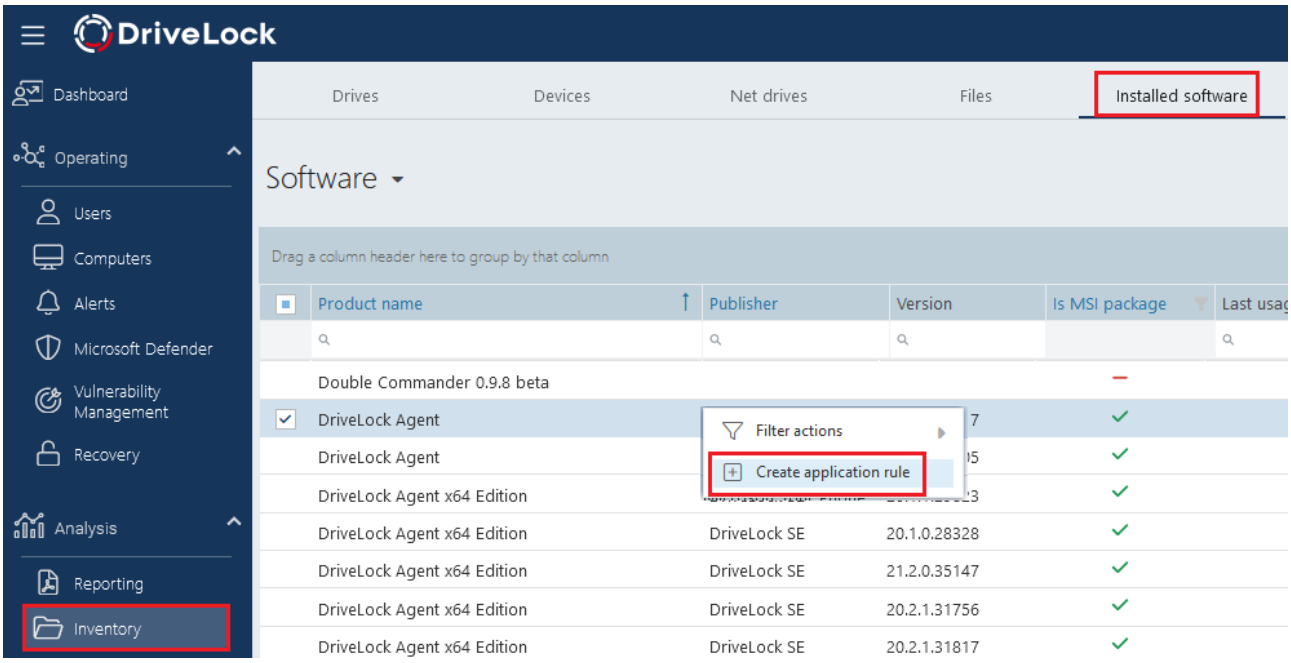


3.6.2.3 Anwendungsregeln über installierte Software erstellen

Wenn für eine Anwendung ausführbare Dateien in der Anwendungsdatenbank vorhanden sind, dann können Sie auch über die installierte Software Anwendungsregeln erstellen. Die Zuordnung von ausführbaren Dateien zur entsprechenden installierten Software geschieht anhand von Ereignissen, die der DriveLock Agent an den DriveLock Enterprise Service (DES) schickt.

Hier gehen Sie genau so vor, wie beim Anlegen von Anwendungsregeln über ausführbare Dateien.





3.7 Berechtigungskonzept im DOC

Das DriveLock Berechtigungskonzept kann nur im DriveLock Operations Center konfiguriert werden. Die Einstellungen im DOC gelten auch für die DMC.

Benutzerkonten und Berechtigungen können im Menü **Einstellungen** in der Ansicht **Berechtigungen** definiert werden.

Konten

Ein Konto enthält die sicherheitsrelevanten Daten eines Benutzers und ermöglicht den Zugriff auf DriveLock-Funktionen. Jedem Konto sind Rollen zugewiesen (Rollenzuweisungen), die verschiedene Rechte (Rollenberechtigungen) zum Ausführen von Aktionen beinhalten.

- Konten im Cloud-Umfeld
  Rollenzuweisungen werden bei den e-Mail-Konten direkt ausgewertet
- Active Directory-Konten
  Bei Active Directory können Konten sowohl für einzelne Benutzer wie auch für Gruppen angelegt werden. Bei der Anmeldung eines Benutzers werden dessen Active Directory-Gruppen aufgelöst und die Rollenzuweisungen des Benutzers werden mit den Rollenzuweisung für alle gefundenen Gruppenkonten ergänzt.
- Azure Active Directory-Konten
  Die Gruppen und Mitgliedschaften eines Azure Active Directory (AAD) können synchronisiert werden. In Kombination mit der Anmeldung per SAML werden die Gruppenzugehörigkeiten des Benutzers vom Azure Active Directory abgefragt. Dies ermöglicht analog zum Active Directory Rollenzuweisungen auf die Azure AD-Gruppen, in denen der Benutzer Mitglied ist.

Rollen und Rollenberechtigungen

- In einer Rolle werden verschiedene Berechtigungen zusammengefasst. Beim Ausführen von Aktionen prüft DriveLock, ob die benötigten Berechtigungen vorliegen.
- DriveLock bietet mehrere eingebaute Rollen an (z.B. Supervisor, Administrator). Sie können aber auch eigene Rollen definieren und verwenden.

Rollenzuweisungen

- Eine Rollenzuweisung verbindet ein Konto mit einer Rolle und optional einem Kontext, der die Anwendung der Rolle und dessen Berechtigungen auf bestimmte Objekte beschränkt.
- Mögliche Kontexte für Rollenzuweisungen:
  - **Global**: die Rolle gilt global ohne Einschränkungen auf Objekte
  - **OU**: die Rolle gilt nur für Computer, die in der ausgewählten Active Directory OU enthalten sind
  - **Gruppe**: die Rolle gilt nur für Computer, die Mitglied in der angegebenen DriveLock Gruppe sind
  - **Richtliniensammlung**: die Rolle gilt nur für Richtlinien, die in einer Richtliniensammlung enthalten sind

> Hinweis: Im Computer-Kontext (OU oder Gruppe) sind nur Berechtigungen auf Computer möglich, selbst wenn die Rolle ursprünglich auch

Berechtigungen zu anderen Bereichen enthält.
Ein Kontext auf Richtliniensammlungen erlaubt nur Berechtigungen auf Richtlinien, aber keine andere Objekte.

- Beispiele:
  - Ein Benutzer mit der Rolle Helpdesk darf im Kontext Global alle Computer und Ereignisse, das gesamte Inventar usw. sehen und auch Richtlinien öffnen (aber nicht speichern).
  - Ein Benutzer mit der Rolle Helpdesk darf im Kontext Active Directory OU nur Computer, Ereignisse usw. sehen, die in der angegebenen Active Directory OU enthalten sind. Dieser Benutzer darf allerdings keine Richtlinien öffnen, da die Rollenzuweisung auf OUs sich nur auf Computer, aber nicht auf Richtlinien bezieht. Eine zusätzliche Rollenzuweisung kann aber hinzugefügt werden, um dies zu ermöglichen.

3.8 Richtliniensammlungen (DOC)

Im DOC haben Sie die Möglichkeit, Richtlinien in Richtliniensammlungen zu gruppieren. Diese Sammlungen können dann in Rollenzuweisungen verwendet werden, um den Zugriff auf bestimmte Richtlinien für eine bestimmte Rolle zu beschränken.

3.9 Datenmaskierung

Durch Aktivierung der Datenmaskierung lassen sich sensible Benutzer- oder Computerdaten im Sinne der Datenschutzgrundverordnung (DSGVO) einfach ausblenden. Statt des Benutzer- oder Computernamens steht dann ein Platzhalter. Die Maskierung verhindert somit eine Auswertung von Benutzerverhalten und kann - bei entsprechender Einstellung - dazu beitragen, Rückschlüsse auf Benutzer von Computern unmöglich zu machen.

Für die Aktivierung bzw. Deaktivierung wird eine spezielle Berechtigung (Rolle) benötigt.

Im Bereich **Unmaskierte Daten anzeigen** können Sie angeben, unter welchen Voraussetzungen die Maskierung der Daten für die jeweils aktuelle Browser-Ansicht temporär aufgehoben werden darf. Für alle anderen Ansichten werden die Daten weiterhin maskiert angezeigt. Dies kann zum Beispiel notwendig sein, wenn dringend systemrelevante Fehler behoben werden müssen oder bei einem Benutzer auffälliges Verhalten festgestellt wurde.

Auch für die Aufhebung der Datenmaskierung bedarf es spezieller Berechtigungen. Zur Wahl stehen hierfür:

- **Mit Rollenberechtigung**: Eine entsprechende Berechtigung muss vorhanden sein.
- **Mit Code**: Die Maskierung kann nur dann aufgehoben werden, wenn ein Code eingegeben wird. Dieser muss gesondert beantragt werden und ist für eine bestimmte Zeit gültig. Diese Option kommt zum Einsatz, wenn niemand Zugriff auf das DOC hat, Daten aber zwingend abgefragt werden müssen, z.B. aus betriebsbedingten Gründen. Der Code muss in diesem Fall wie ein Kennwort behandelt, geheimgehalten und vor Ort eingegeben werden.
- **Mit Genehmigung durch**: Bei dieser Option muss eine Kontaktperson die Genehmigung für die Aufhebung geben. Im Textfeld unten können die entsprechenden Angaben eingetragen werden (z.B. Name, Telefonnummer, E-Mail-Adresse). Dies wird ebenfalls im DOC durchgeführt. Hier wird dann eine Anfrage geschickt und entsprechend darauf reagiert (Genehmigung oder Ablehnung).

Im Bereich **Umfang der Datenmaskierung** geben Sie an, welche Daten maskiert werden sollen.

- **Vollständig**: Alles Benutzer- und Computerdaten werden maskiert. Es werden weder verbundene Entitäten ('Related Entities'), noch Informationen in Ereignissen, Alerts oder in Security Awareness-Sessions angezeigt. Rückschlüsse sind weder auf Computer, noch auf Benutzer möglich. Diese Option bietet zwar den höchsten Datenschutz, erschwert aber unter Umständen aber auch die Problembehebungen.
- **Nur Benutzernamen**: Wenn mehrere Benutzer auf Computern arbeiten, kann diese Option hilfreich sein. Es werden nur noch die Computernamen angezeigt, die Benutzernamen sind maskiert. Für die Problembehebung ist diese Variante gut einsetzbar.
- **Individuell**: Klicken Sie auf **Konfigurieren**, um anzugeben, in welchem Kontext und bei welchen Ereignissen Benutzer- bzw. Computerdaten maskiert werden sollen. Mit diesen Einstellungen können Sie die Datenmaskierung präzise konfigurieren und beispielsweise auf verschiedene Ereignisse beschränken.

Auf dem Reiter **Allgemein** können Sie folgende Optionen auswählen:

- **Computer des Benutzers anzeigen**: Wenn Sie diese Option aktivieren, werden die Computer eines maskierten Benutzers unter **Zugehörige Objekte** in der Ansicht **Benutzer** (**Endbenutzer auf verwalteten Computern**) angezeigt. Beachten Sie, dass dies unter Umständen eine Rückverfolgung des Benutzers über den jeweiligen Computer zulässt.
- **'Letzter angemeldeter Benutzer' in Klartext anzeigen**: Wählen Sie diese Option, wird der Name des Benutzers in der Ansicht **Computer** in der Spalte **Letzter**

angemeldeter Benutzer angezeigt, der als letztes an diesem Computer angemeldet war.

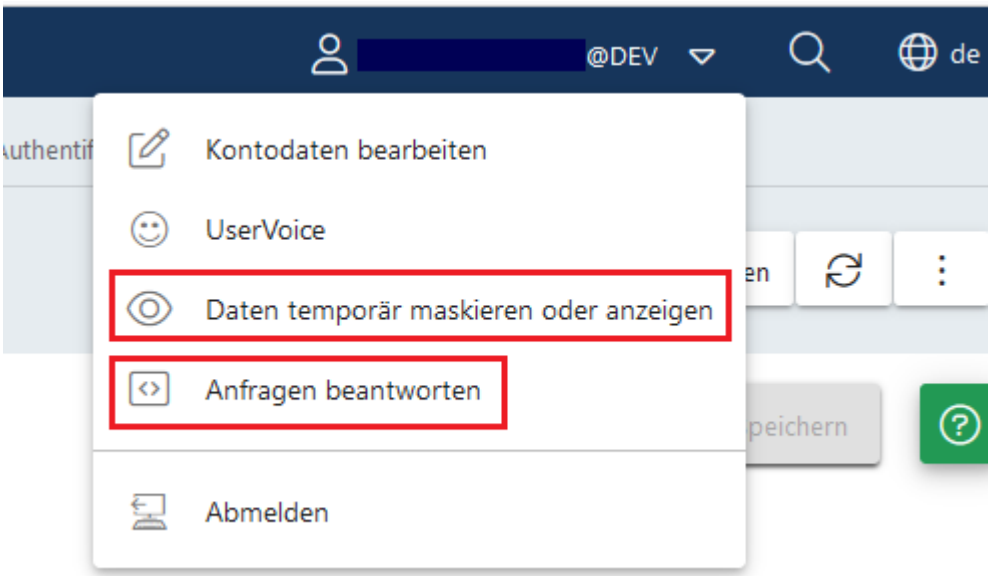
- **'Integrierter Benutzer' in Klartext anzeigen**: Bei Aktivierung dieser Option werden die Betriebssystemkonten in allen Ansichten angezeigt, z.B. NT-AUTHORITY\SYSTEM. Diese Option ist standardmäßig ausgewählt.
- Des weiteren können Sie wählen, in welchem **Kontext** die Datenmaskierung angewendet werden soll, z.B. bei Security-Awareness-Sessions.

Auf dem Reiter **Ereignisse** können Sie gezielt einzelne oder mehrere Ereignisse auswählen, bei denen Daten maskiert werden sollen.

Weitere Optionen der Datenmaskierung (s. Abbildung):

Mit der Schaltfläche **Anfragen beantworten** können Sie Anfragen zur Aufhebung der Datenmaskierung genehmigen oder ablehnen.

Diese Option kann auch vom Kontextmenü des Benutzers aus gewählt werden (s. Abbildung). Hier befindet sich auch die Option zur Umkehrung der Datenmaskierung. Wenn Daten bereits maskiert sind, kann eine Anfrage zur temporären Aufhebung hier gestellt werden, oder im umgekehrten Fall eine schnelle Datenmaskierung (jeweils für Computer- und/oder Benutzerdaten) angefordert werden.



Anwendung der Datenmaskierung bei gesetztem Filter "Benutzername"

Wenn in einem Widget der Filter **Benutzername** gesetzt und gleichzeitig die Datenmaskierung aktiviert ist, werden keine Daten angezeigt. Eine Ausnahme stellt der Systembenutzer dar. Dieser wird mit Hilfe der Eingeschaft Ist Systembenutzer gesetzt.

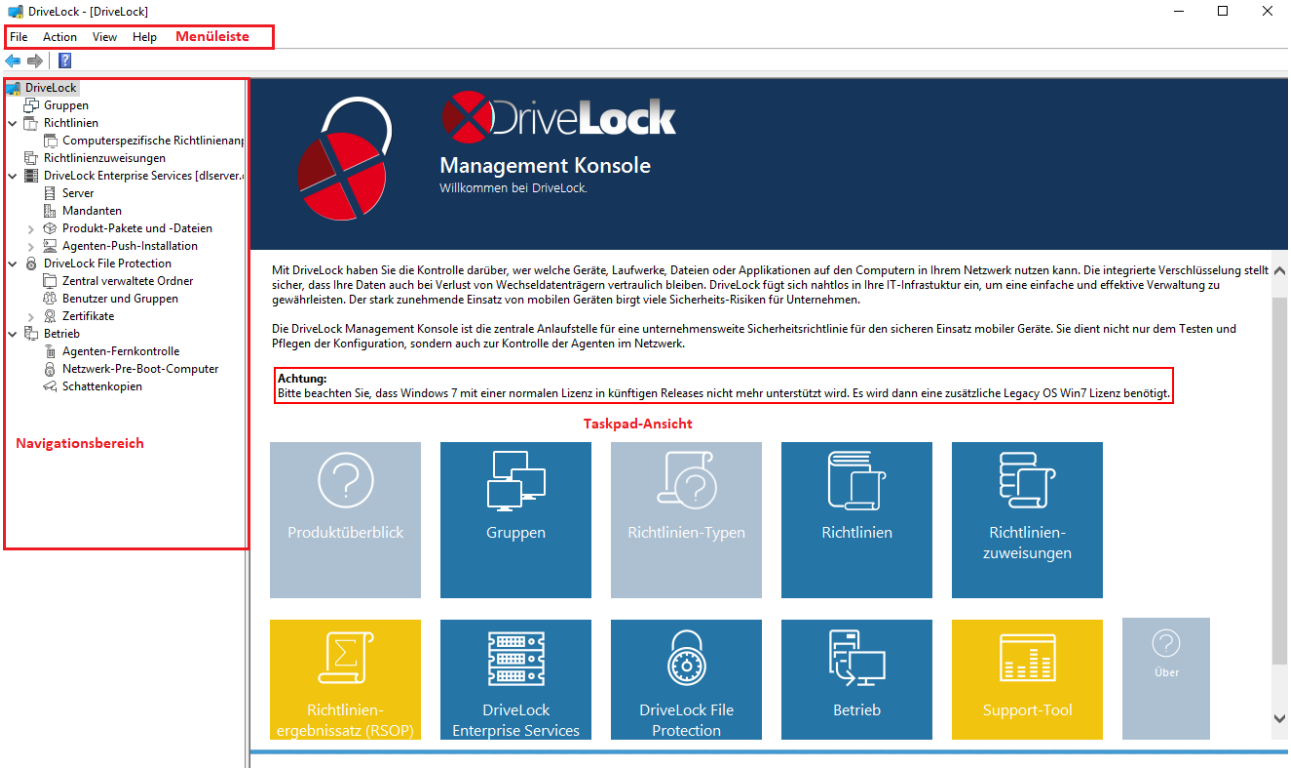
4 DriveLock Management Konsole (DMC)

Die DriveLock Management Konsole (DMC) ist ein sogenanntes MMC Snap-In und kann damit sowohl als eigenständige Konsole sowie als zusätzlicher Bestandteil einer bestehende administrativen Zusammenstellung in einer Microsoft Management Console (MMC) verwendet werden.

In der DriveLock Management Konsole (DMC) erledigen Sie die wichtigsten Konfigurationsaufgaben. Diese sind:

- DriveLock Gruppen erstellen,
- Richtlinien anlegen,
- Richtlinien zuweisen,
- DriveLock Enterprise Services konfigurieren,
- DriveLock File Protection konfigurieren und den
- Betrieb der DriveLock Agenten kontrollieren.

Nach der Installation der DriveLock Management Konsole können Sie diese über das Windows Startmenü unter **Alle Programme / DriveLock / DriveLock Management Konsole** starten:



Am oberen Rand befindet sich die Menüleiste und enthält das Standardmenü einer MMC, sowie die Schaltflächen für den Schnellzugriff auf bestimmte Funktionen.

Links im Navigationsbereich können die verschiedenen Funktionen der DriveLock Management Konsole erreicht werden. Die Baumstruktur enthält einzelne Knoten mit Unterfunktionen.

Die Taskpad-Ansicht auf der rechten Seite zeigt die innerhalb eines Knotens verfügbaren Menüpunkte. Diese Ansicht kann auch zu einer Detailansicht (**Listenansicht**) wechseln, wenn Elemente des untersten Knotens in einer Listendarstellung angezeigt werden. Diese Darstellung entspricht weitgehend der sogenannten klassischen Ansicht einer MMC.

Fast jeder Knoten im Navigationsbereich und jedes Element einer Detailansicht hat ein Kontextmenü mit entsprechenden Funktionen, das durch einen Rechtsklick geöffnet wird.

An manchen Stellen der DriveLock Management Konsole bzw. im Richtlinien-Editor können Sie von der Taskpad-Ansicht zur **Listenansicht** wechseln. Über das **Kontextmenü / Ansicht / Taskpad-Ansicht** wechseln Sie wieder zurück.

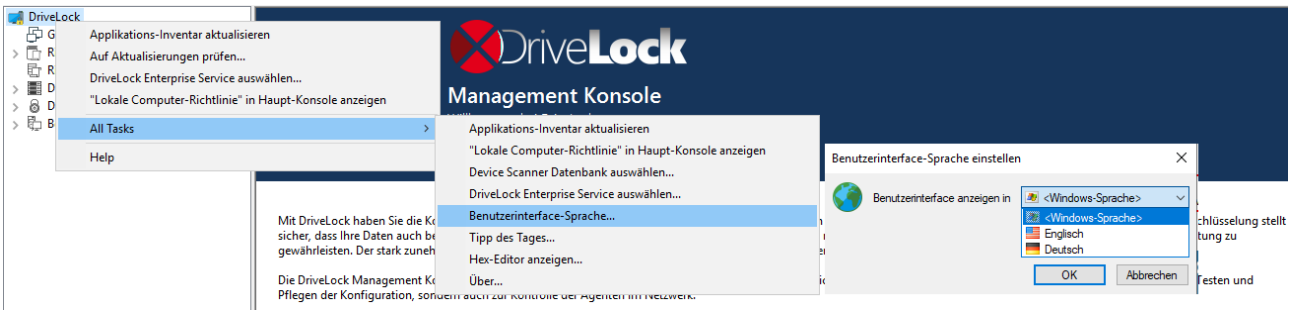
4.1 Allgemeine Hinweise

4.1.1 Ändern der Sprache der Benutzeroberfläche

Rechts-klicken Sie auf DriveLock und wählen Sie **Alle Aufgaben-> Benutzerinterface-Sprache**.

> Hinweis: Je nach Wahl der Betriebssystem-Sprache werden einige Standardschaltflächen und -menüpunkte in dieser Sprache angezeigt und nicht in der, die Sie in DriveLock als Benutzerinterface-Sprache auswählen.

So wählen Sie Ihre gewünschte Sprache:



4.2 Richtlinien

4.2.1 Verteilung der DriveLock Konfigurationseinstellungen

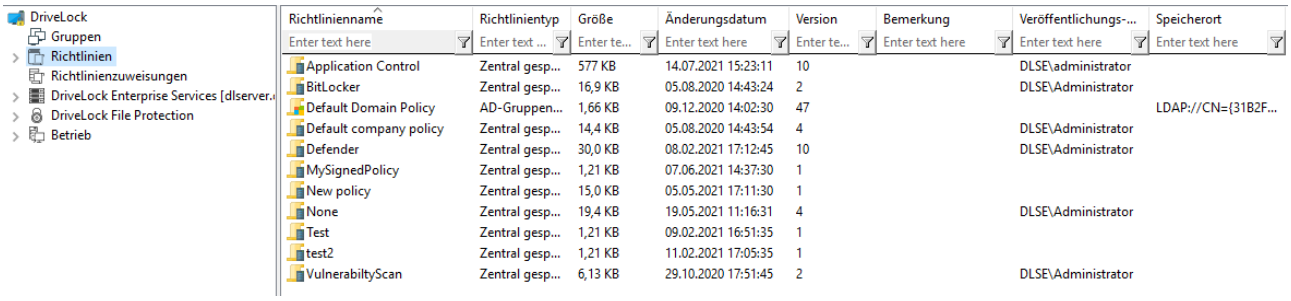
Es gibt verschiedene Arten, Konfigurationseinstellungen an Clients zu verteilen. Die Schritte zur Konfiguration von Einstellungen sind in allen Arten von Richtlinien identisch. Sie können dieselben Parameter, Whitelist-Regeln oder Netzwerkeinstellungen konfigurieren.

Die folgende Konfigurationsmatrix hilft Ihnen einen Überblick zu bekommen, welche Konfigurationsart für Sie am besten geeignet ist:

	Zentrale Konfiguration	Benötigt zwingend einen DES	Nutzt vorhandene Infrastruktur	Historie / Versionierung	Flexibilität
Zentral gespeicherte Richtlinie (CSP)	Ja	Ja	Nein	Ja	Sehr gut
Gruppenrichtlinie	Ja	Nein	Ja (AD)	Nein	Befriedigend
Konfigurations-Datei	Ja	Nein	Ja (UNC, http, ftp)	Nein	Nein
Lokale Richtlinie	Nein	Nein	Nein	Nein	Nein

Achtung: Bevor Sie Einstellungen an mehrere Clients im Netzwerk verteilen, sollten Sie diese erst auf einem oder mehreren Test-Clients testen.

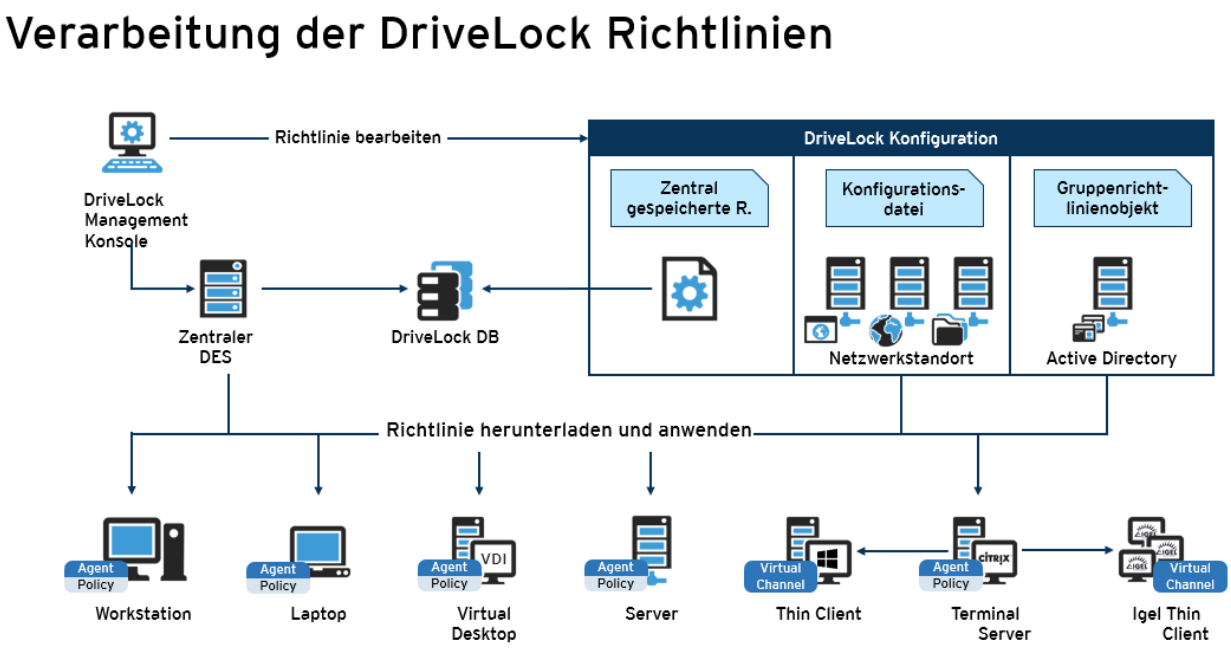
Konfigurationseinstellungen werden in der DriveLock Management Konsole unter Richtlinien verwaltet:



Richtlinienname	Richtlinientyp	Größe	Änderungsdatum	Version	Bemerkung	Veröffentlichungs-...	Speicherort
Application Control	Zentral gesp...	577 KB	14.07.2021 15:23:11	10		DLSE\administrator	
BitLocker	Zentral gesp...	16,9 KB	05.08.2020 14:43:24	2		DLSE\Administrator	
Default Domain Policy	AD-Gruppen...	1,66 KB	09.12.2020 14:02:30	47			LDAP://CN={31B2F...
Default company policy	Zentral gesp...	14,4 KB	05.08.2020 14:43:54	4		DLSE\Administrator	
Defender	Zentral gesp...	30,0 KB	08.02.2021 17:12:45	10		DLSE\Administrator	
MySignedPolicy	Zentral gesp...	1,21 KB	07.06.2021 14:37:30	1			
New policy	Zentral gesp...	15,0 KB	05.05.2021 17:11:30	1			
None	Zentral gesp...	19,4 KB	19.05.2021 11:16:31	4		DLSE\Administrator	
Test	Zentral gesp...	1,21 KB	09.02.2021 16:51:35	1			
test2	Zentral gesp...	1,21 KB	11.02.2021 17:05:35	1			
VulnerabiltyScan	Zentral gesp...	6,13 KB	29.10.2020 17:51:45	2		DLSE\Administrator	

Architektur

In der folgenden Grafik sehen Sie, wie die Konfigurationseinstellungen verteilt werden:



> Achtung: Es wird empfohlen, dass bei Verwendung von Microsoft Gruppenrichtlinien auch das Berechtigungskonzept von Gruppenrichtlinien verwendet wird, um sicherzustellen, dass nur autorisierte Administratoren die DriveLock Konfigurationsrichtlinie einsehen bzw. verändern können. Wenn Sie Konfigurationsdateien verwenden, benutzen Sie die Windows Dateizugriffsberechtigungen hierfür. Bei zentral gespeicherten Richtlinien sorgt die Zugriffskontrolle auf den DriveLock Enterprise Service für entsprechende Sicherheit.

4.2.2 Zentral gespeicherte Richtlinien

Zentral gespeicherte Richtlinien (CSP = Centrally Stored Policy) sind in der DriveLock Datenbank abgespeichert und werden über den DriveLock Enterprise Server (DES) an die Agenten verteilt.

Für die meisten Anwendungsfälle bieten sich aus folgenden Gründen CSPs an:

- CSPs unterstützen eine Versionierung und Änderungsverfolgung und können vom Administrator getrennt bearbeitet oder veröffentlicht werden.
- Mehrere CSPs können auf einen Agenten zugewiesen werden (was z.B. bei Konfigurationsdateien nicht der Fall ist).
- CSPs können in beinahe jeder Netzwerkumgebung, einschließlich Active Directory, Workgroups und Novell Directory Service verwendet werden.

Für Managed Security Service Provider (MSSP) sind CSPs daher die beste Wahl, um Richtlinien der verschiedenen Mandanten zu trennen.

Achtung: Für die Verwendung der zentral gespeicherten Richtlinien ist ein DriveLock Enterprise Service (DES) Voraussetzung.

Sie können eine oder mehrere CSPs an Computer, DriveLock Gruppen, AD Gruppen, OUs oder auch an Alle Computer zuweisen. CSPs können entweder dem Standard-Mandanten (root) oder jedem anderen Mandanten gehören. Der Agent kennt die DES Server, von denen er CSPs beziehen kann. Auf diese Weise lassen sich CSPs mit verschiedenen Einstellungen kombinieren, z.B. enthält eine CSP nur Grundeinstellungen, die dann an alle Clients verteilt werden, und eine andere enthält spezielle Einstellungen, die nur an Clients in einer bestimmten Abteilung zugewiesen werden. So kann man z.B. auch eine CSP erstellen, in der USB-Sticks vom Marketing eingetragen werden, so dass diese CSP dann auch nur von den Marketing-Clients verwendet wird.

Beispiel:

Reihenfolge/Name	Zuweisungsziel	Beschreibung
1. Lizenz-Richtlinie	Alle Computer	Enthält Lizenzinformationen für alle Computer
2. Default_All	Alle Computer	Standard-Einstellungen für alle Computer
3. USB-Sticks Marketing	Marketing-Clients	Freigegebene USB-Sticks für Marketing
4. Festplattenschutz Laptop	Laptops	Festplattenverschlüsselung
5. Anwendungskontrolle Server	Server	Zulässige Anwendungen für

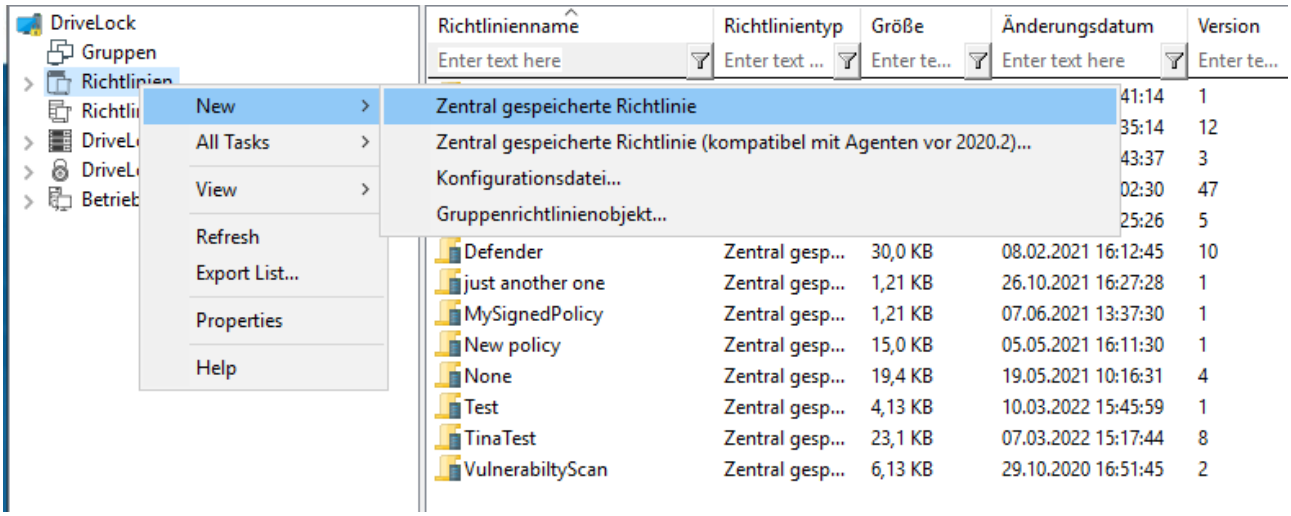
Reihenfolge/Name	Zuweisungsziel	Beschreibung
		Server

4.2.2.1 Richtlinien erstellen und bearbeiten (DMC und DOC)

In der DriveLock Management Konsole (DMC)

Um eine neue zentral gespeicherte Richtlinie für den Mandanten Root oder andere Mandanten anzulegen, rechtsklicken Sie **Richtlinien**, wählen Sie **Neu** und dann **Zentral gespeicherte Richtlinie...**.

> Hinweis: Wenn Sie mit DriveLock Agenten arbeiten, auf denen eine ältere DriveLock Versionen als Version 2020.2 installiert ist, wählen Sie bitte die Option **Zentral gespeicherte Richtlinie (kompatibel mit Agenten vor 2020.2)...** . Diese Agenten können das neue Richtlinienformat noch nicht verstehen.



Vergeben Sie einen Namen, wählen Sie einen Mandaten aus und geben Sie eine kurze Beschreibung des Zwecks der Richtlinie ein.

Markieren Sie ggf. **Bestehende Richtlinie als Vorlage verwenden** und wählen Sie eine Richtlinie aus von der Sie eine Kopie erstellen möchten.

Klicken Sie **OK**, um die neue Richtlinie zu speichern.

Danach öffnet sich der DriveLock Richtlinien-Editor, in dem Sie die neue Richtlinie bearbeiten können.

Wenn Sie eine bereits vorhandene Richtlinie bearbeiten wollen, rechtsklicken Sie auf die Richtlinie und wählen **Bearbeiten**.

Achtung: Denken Sie daran, die Lizenzinformation bei den globalen Einstellungen anzugeben.

Hinweis: Mit Hilfe der Import und Export Funktionen können Einstellungen zwischen einer zentral gespeicherten Richtlinie und einer lokalen Richtlinie ausgetauscht werden.

Im DriveLock Operations Center (DOC)

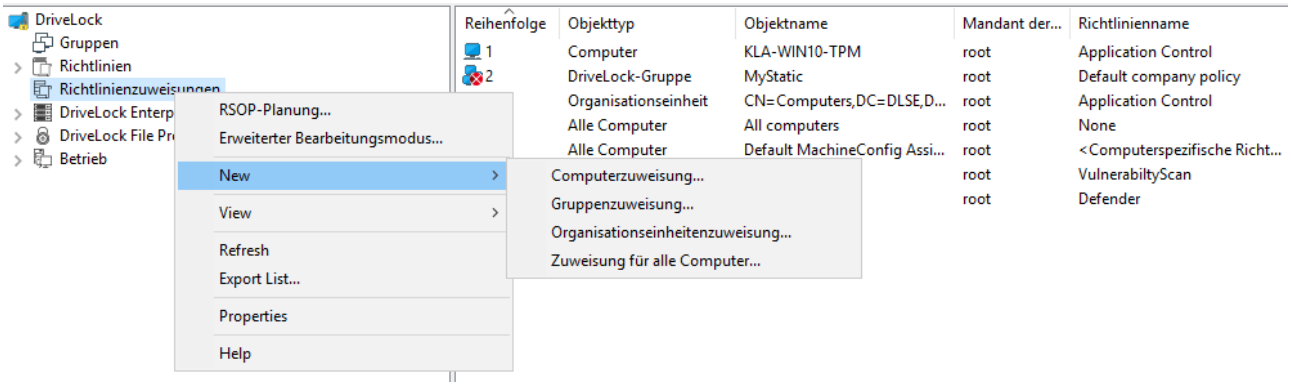
Öffnen Sie im Menü **Konfiguration** die Ansicht **Richtlinien** . Klicken Sie die Schaltfläche **Richtlinie erstellen**. Dann startet der DOC Companion, falls dieser noch nicht läuft. Anschließend öffnet sich der Richtlinien-Editor der DMC und Sie können die Richtlinie bearbeiten, speichern, veröffentlichen und dann direkt im DOC zuweisen. Weitere Informationen finden Sie in der separaten DOC Companion Dokumentation auf DriveLock Online Help.

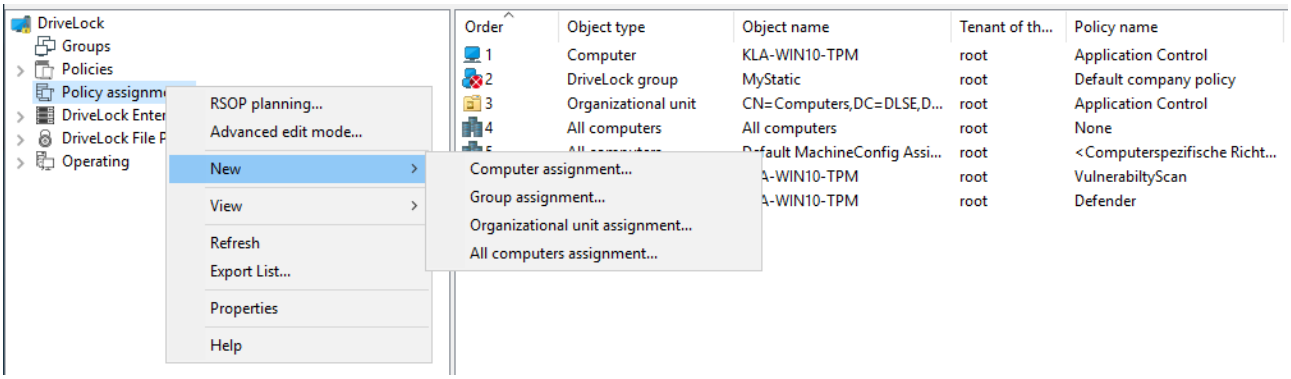
4.2.2.2 Richtlinien zuweisen (DMC und DOC)

In der DriveLock Management Konsole (DMC)

Nachdem Sie eine zentral gespeicherte Richtlinie erstellt und konfiguriert haben, weisen Sie sie bestimmten oder allen Computern, Gruppen, DriveLock-Gruppen oder Organisationseinheiten (OUs) zu, für die sie wirksam sein soll.

Hinweis: Bevor Sie statische und dynamische DriveLock-Gruppen für Richtlinienzuweisungen verwendet werden können, müssen diese zuerst definiert worden sein. Nach erfolgter Zuweisung der DriveLock-Gruppe zu einer Richtlinie erscheint sie im Reiter Zuweisungen in den Gruppeneigenschaften.

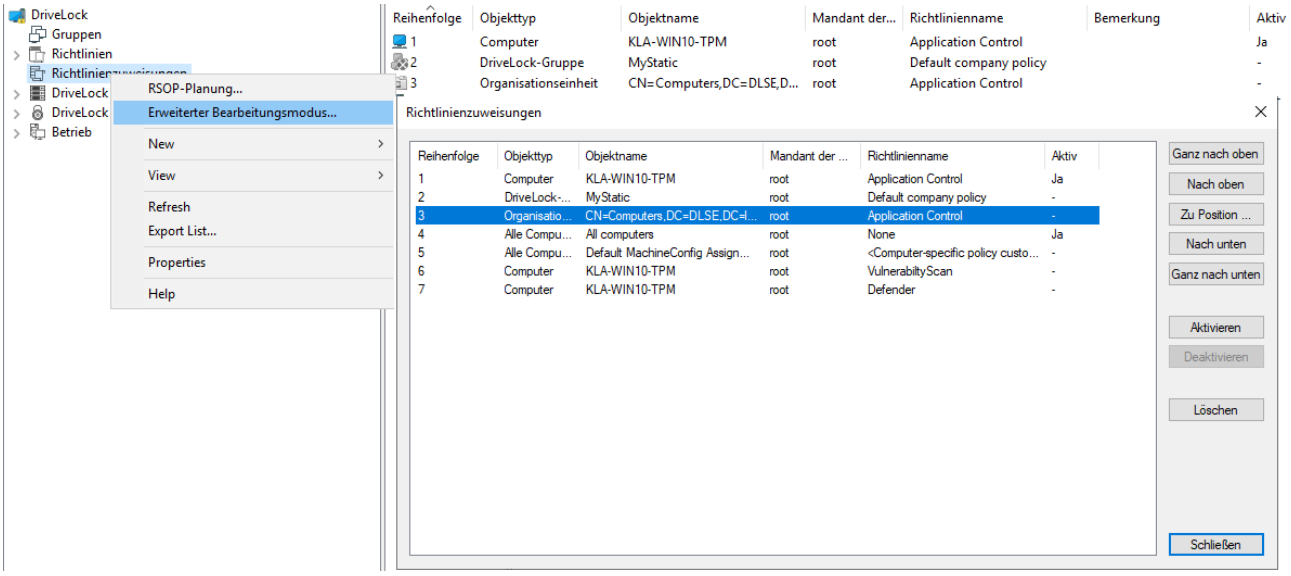




Im Zuweisungsdialog geben Sie die gewünschten Computer, Gruppen oder OUs an und wählen einen Mandanten und die passende Richtlinie aus. Richtlinien, die für den Root-Mandanten gespeichert sind, können mit jedem Mandanten verwendet werden, während Richtlinien die für eine bestimmten Mandaten abgelegt sind, nur diesem Mandanten zugeordnet werden können.

Um die Reihenfolge anzupassen, rechtsklicken Sie auf einen Eintrag und verschieben diesen.

Wenn Sie mehr als eine Richtlinie auf einmal verschieben bzw. bearbeiten möchten, klicken Sie **Erweiterter Bearbeitungsmodus...** und bewegen die Richtlinie an die gewünschte Stelle. Hier können Sie die Richtlinien auch deaktivieren oder löschen.



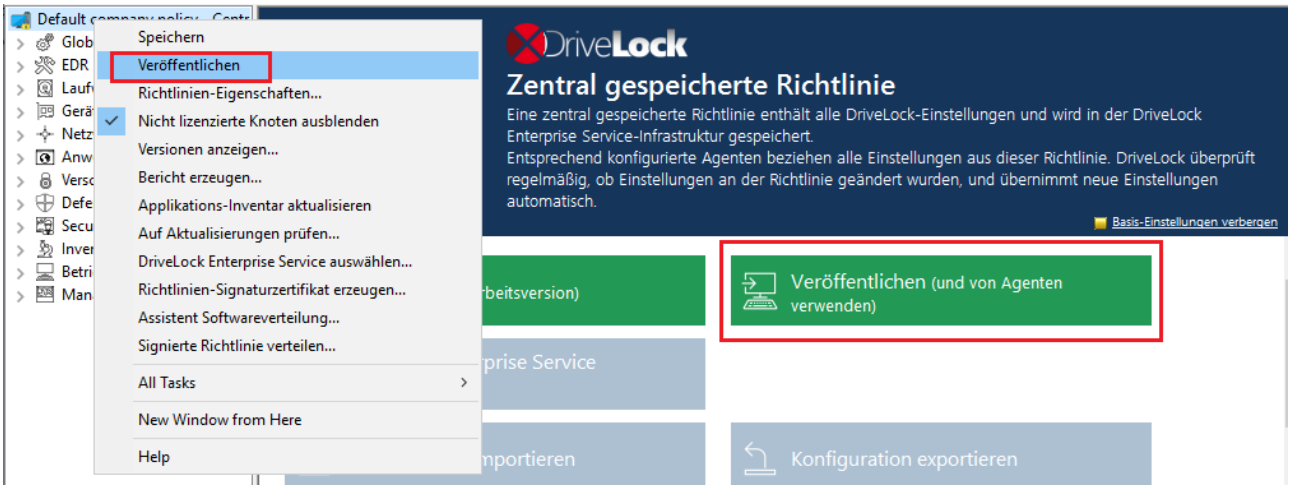
Im DriveLock Operations Center (DOC)

Auf dem Reiter **Richtlinienzuweisungen** (im Menü **Konfiguration**, Ansicht **Richtlinien**) können Sie analog zur DMC Richtlinienzuweisungen erstellen, bearbeiten, durch Drag and Drop an die gewünschte Stelle verschieben und aktivieren bzw. deaktivieren.

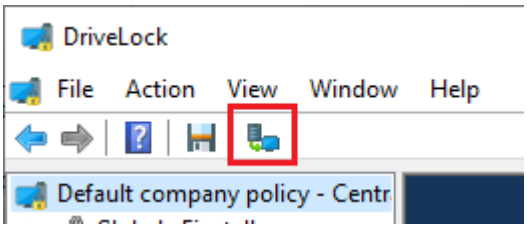
Auch im DOC haben Sie die Möglichkeit, eine Richtlinie allen Computern (diese Option ist standardmäßig aktiviert) oder bestimmten Zielen (AD-Computer, DriveLock-Gruppen, Azure AD-Gruppen. AD-Gruppen oder OU-Containern) zuzuweisen.

4.2.2.3 Richtlinien veröffentlichen

Um eine Richtlinie wirksam zu machen, muss die geänderte Richtlinie zunächst veröffentlicht werden. Wählen Sie dazu entweder den Kontextmenübefehl oder die Schaltfläche in der Taskpad-Ansicht:



Oder ganz einfach in der Menüleiste mit folgendem Symbol:



Geben Sie optional im Dialog einen **Veröffentlichungs-Kommentar** ein und bestätigen Sie die Veröffentlichung mit OK.

Wenn Sie die Richtlinie **Im neuen Format speichern**, kann sie nur von Agenten, die mit einer DriveLock Version ab 2020.2 installiert sind, verstanden werden. Das neue Richtlinienformat sorgt für bessere Leistung (schnellere Verarbeitung der Richtlinien, weniger Datenverkehr zwischen DES und Agenten).

> Hinweis: Gegebenenfalls können Sie die Richtlinie auch signieren und das entsprechende Signaturzertifikat verwenden im Veröffentlichungsdialog auswählen.

4.2.3 Gruppenrichtlinienobjekt

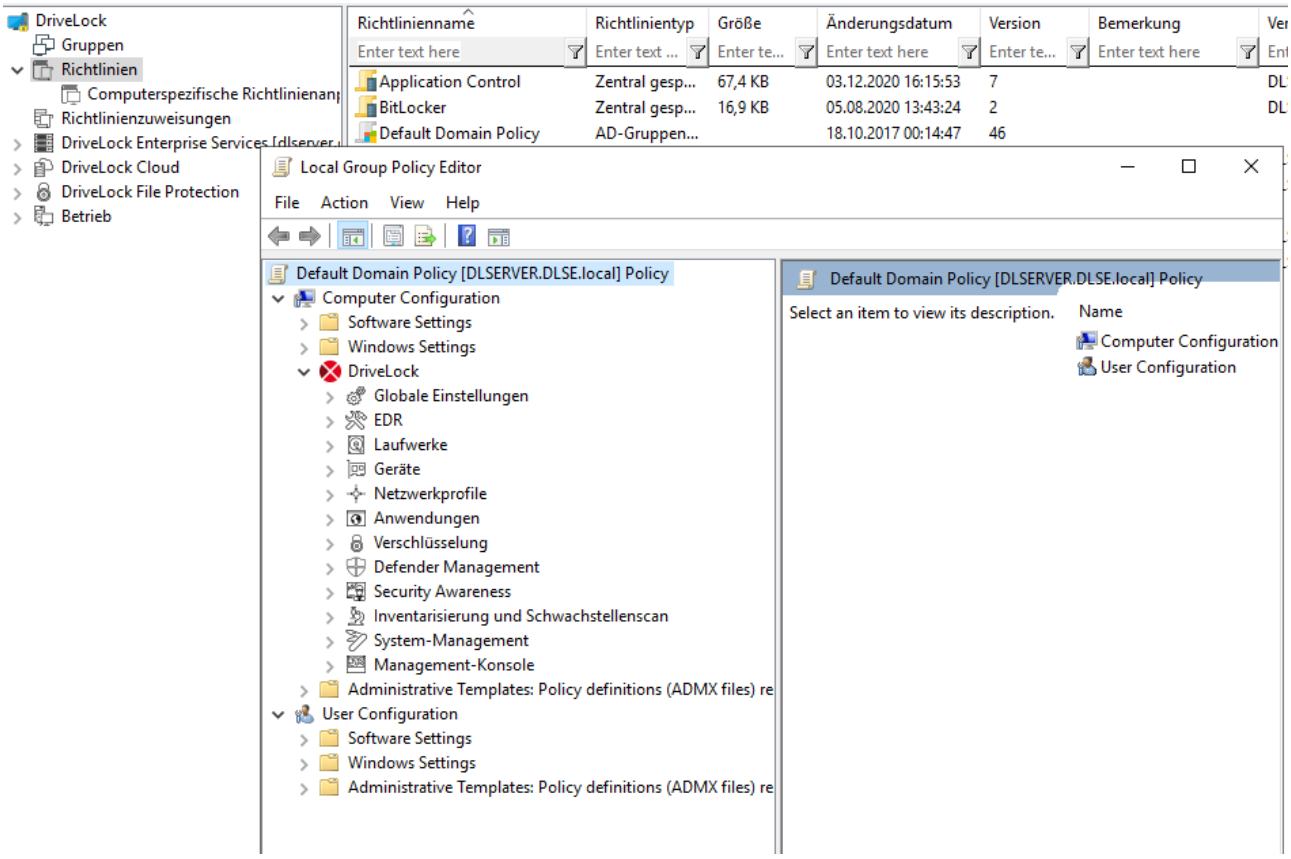
Eine andere Möglichkeit, um den DriveLock Agenten auf mehreren Rechnern zu konfigurieren, ist die Nutzung von Active Directory Gruppenrichtlinien. DriveLock kann mit dem Gruppenrichtlinieneditor in Verbindung mit dem DriveLock Managment Konsole (MMC) Snap-In konfiguriert werden. Dieses Snap-In ist Bestandteil einer DriveLock Komplettinstallation.

DriveLock nutzt Gruppenrichtlinien, um Einstellungen an Rechner zu verteilen, die zu einer Active Directory Domain gehören. Der auf diesen Rechnern laufende DriveLock Agent wendet alle Einstellungen an, die in diesen Gruppenrichtlinien definiert sind.

In einer Active Directory Umgebung sind Rechner in Organisationseinheiten angeordnet (OUs) um gemeinsame identische Einstellungen umzusetzen; es ist daher gängige Praxis, Gruppenrichtlinien – die DriveLock Einstellungen beinhalten – OU's zuzuweisen. Ein weiterer Grund für die Nutzung von OUs ist die Möglichkeit zur Delegierung administrativer Aufgaben. Die Zuweisung von Gruppenrichtlinien zu OUs anstelle der ganzen Active Directory Domain oder Site ist ebenfalls empfehlenswert, da so geeignete Sicherheitslevel für jede Abteilung definiert werden können.

Um existierende oder neue Gruppenrichtlinien hinzuzufügen, die DriveLock Einstellungen beinhalten, rechts-klicken Sie auf Richtlinien -> Neu/New -> Gruppenrichtlinienobjekt hinzufügen..., um die Gruppenrichtlinie der MMC hinzuzufügen.

Danach wählen Sie die entsprechende GPO und klicken Bearbeiten. Es öffnet sich ein neues Fenster mit dem Microsoft GPO Editor, mit dem die Einstellungen bearbeitet werden können.



Das DriveLock Snap-In zeigt die gleichen Objekte in der Konsole wie bei einer lokalen Konfiguration.

Konfigurationsänderungen werden von dem DriveLock Agenten direkt nach Anwendung der Gruppenrichtlinien durch Windows entdeckt. Dies kann bis zu 30 Minuten nach Erstellung der Richtlinie dauern. Um Änderungen an Richtlinien sofort zu übernehmen, kann eine Aktualisierung der Gruppenrichtlinie initiiert werden. Dazu wird auf Kommandozeilenebene einer der folgenden Befehle ausgeführt (welcher auch über die Agentenfernkontrolle aktiviert werden kann): `gpupdate /force`

4.2.4 Konfigurationsdateien

Anstelle von Gruppenrichtlinien oder zentral gespeicherten Richtlinien kann DriveLock auch in anderen Betriebssystemumgebungen als Windows (z.B. Novell NetWare) zentral konfiguriert werden.

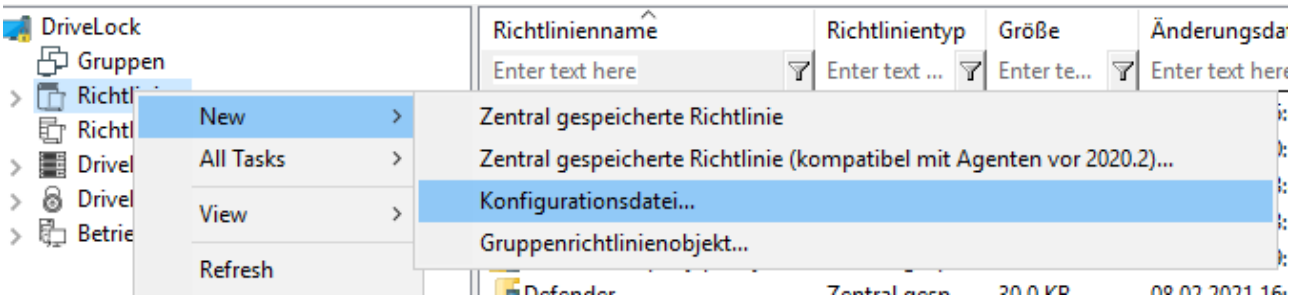
In Systemumgebungen ohne Active Directory und einen DriveLock Enterprise Service können die DriveLock Einstellungen mittels Konfigurationsdatei verteilt werden. Auf diese Datei kann auf einem zentralen Netzlaufwerk unter Nutzung eines UNC Pfades oder per HTTP/FTP zugegriffen werden.

Die Nutzung von Konfigurationsdateien ist der Nutzung von Gruppenrichtlinien sehr ähnlich. Benutzerspezifische Einstellungen sind allerdings beschränkt, wenn keine zentrale Benutzerdatenbank wie bei Active Directory zur Verfügung steht. Es können jedoch lokale Benutzer oder Gruppen in den Einstellungen verwendet werden. Eine Anbindung an Novell eDirectoy ist vorhanden.

Sie müssen den DriveLock Agenten so konfigurieren, dass er seine Konfigurationseinstellungen von einer Konfigurationsdatei bezieht. Um dies durchzuführen, enthält DriveLock einen Software Verteilungsassistenten, der eine angepasste MSI oder MST Datei erstellen kann.

Weitere Informationen über die Nutzung von DriveLock in einem Novell Netzwerk befinden sich im Whitepaper "WP - DriveLock in Novell Umgebungen.pdf" (erhältlich auf Nachfrage).

Rechtsklicken Sie auf **Richtlinien**, wählen Sie **Neu** und dann **Konfigurationsdatei...**.



DriveLock fordert daraufhin die Eingabe des Namens und Pfads der neuen Konfigurationsdatei und öffnet ein neues DriveLock Management Konsolenfenster, in dem die neuen Richtlinieneinstellungen konfiguriert werden können.

Auch hier haben Sie die Möglichkeit, eine Konfiguration aus einer Datei zu importieren oder einen Export in eine Datei durchzuführen.

Achtung: Denken Sie daran, die Lizenzinformation bei den globalen Einstellungen anzugeben.

Hinweis: Mit Hilfe der Import und Export Funktionen können Einstellungen zwischen einer Gruppenrichtlinie und einer lokalen Konfiguration ausgetauscht werden.

Um eine bestehende Konfigurationsdatei zu öffnen, rechts-klicken Sie auf **Richtlinien**, wählen dann **Alle Aufgaben/All Tasks** und dann **Konfigurationsdatei öffnen...**. Die Konfigurationsdatei erscheint auf der rechten Seite.

Wählen Sie die Datei und klicken Sie Bearbeiten, um ein neues DriveLock Management Konsolenfenster zu öffnen.

> Hinweis: Das DriveLock Management Konsolenfenster sichert Änderungen der Konfiguration automatisch, wenn das Fenster geschlossen wird

Nachdem die Einstellungen komplett sind, kann die Konfiguration durch Kopieren der Konfigurationsdatei auf die zentrale Netzwerkfreigabe, von der die Clients die Einstellungen beziehen, verfügbar gemacht werden.

Der DriveLock Agent kann auf Konfigurationsdateien folgendermaßen zugreifen:

- UNC: z.B. \\myserver\share$\drivelock\dlconfig.cfg
- FTP: z.B. myserver/pub/drivelock/dlconfig.cfg
- HTTP: z.B. http://myserver/drivelock/dlconfig.cfg

In Umgebungen ohne Active Directory (wie beispielsweise Novell NetWare) muss der Ort der Konfigurationsdatei während der Agenteninstallation angegeben werden.

> Hinweis: Sie sollten eine anfängliche Konfigurationsdatei vor dem Verteilen der Agenten erstellen und den Pfad dieser Datei während der Installation mittels Kommandozeile oder angepasster Installationsdatei angeben.

Der DriveLock Agent liest die Konfigurationsdatei während der Installation aus und beginnt mit der Umsetzung der darin enthaltenen Einstellungen.

> Achtung: Bei der Nutzung von Konfigurationsdateien prüft der Agent diese nur beim Start auf Änderungen und zu festgelegten Intervallen, die definiert werden können.

Bei der Installation des DriveLock Agenten müssen Sie die Informationen, von wo der Agent seine Konfiguration laden soll, mit angeben. Das geht am einfachsten über den Softwareverteilungs-Assistenten. Öffnen Sie diesen durch rechtsklicken auf **Richtlinien**, dann **Alle Aufgaben** und **Konfigurationsdatei verteilen...**.

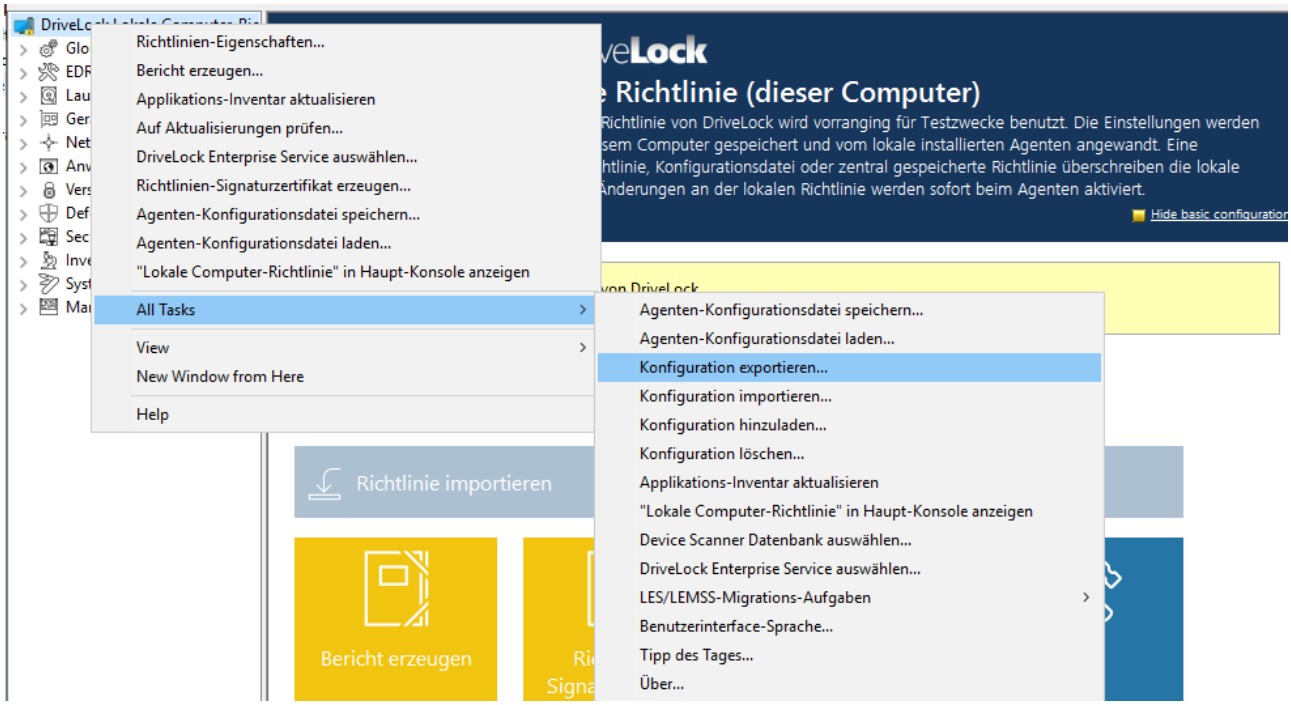
4.2.5 Lokale Konfiguration

Eine lokale Konfiguration wird nur auf dem Rechner angewendet, auf dem sich die DriveLock Management Konsole befindet. Sie eignet sich dafür, bestimmte Richt-

linieneinstellungen auf einem einzelnen Computer mit installiertem DriveLock Agenten zu testen, bevor Sie weitere Richtlinien auf weitere Agenten in ihrem Netzwerk verteilen.

Um die lokalen Einstellungen zu konfigurieren, öffnen Sie das **Startmenü** -> **Alle Programme** -> **DriveLock** und wählen dann **DriveLock Lokale Richtlinie**. Der Richtlinien-Editor öffnet sich.

Wenn Sie die lokale Konfiguration in einer anderen Richtlinie nutzen oder diese sichern wollen, muss diese zuerst in eine Datei exportiert werden. Öffnen Sie das Kontextmenü des obersten Knotens und wählen Sie dann unter **Alle Aufgaben** den Menübefehl **Konfiguration exportieren...**. Geben Sie dann ein Verzeichnis und einen Dateinamen an und speichern Sie die lokale Konfigurationsdatei. Diese hat die Endung .dlr.



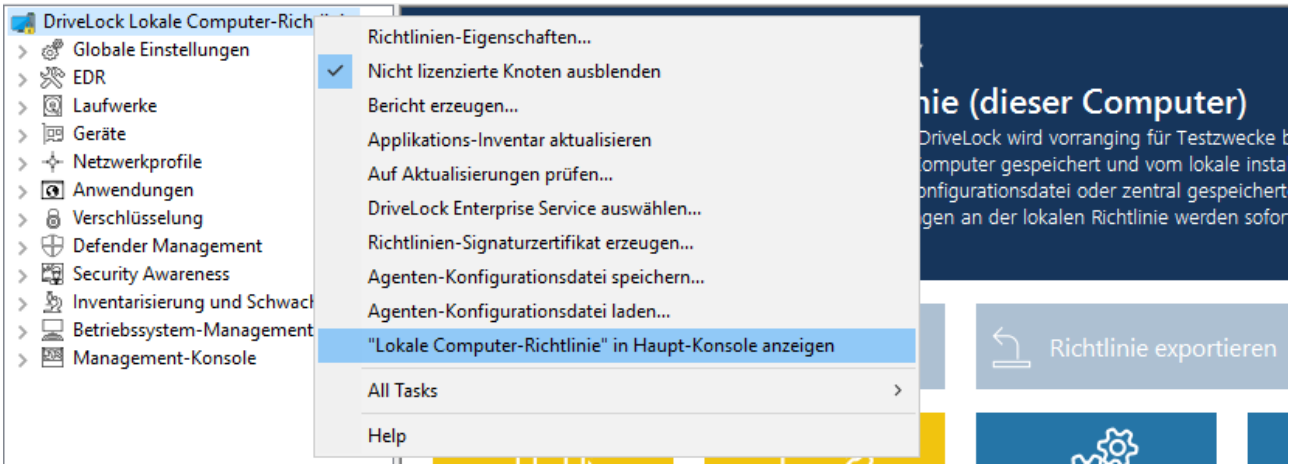
> Hinweis: Sie können eine lokale Konfiguration auch importieren, wenn Sie beispielsweise zuvor eine Richtlinie aus einer Gruppenrichtlinie exportiert und dann in eine lokale DriveLock Konfiguration importiert haben.

Weitere Optionen:

Agenten-Konfigurationsdatei speichern: Mit diesem Befehl wird eine Agenten-Konfigurationsdatei (.cfg) erstellt. Die Datei kann zur Verteilung einer DriveLock Konfiguration ohne Gruppenrichtlinien verwendet werden oder in einem Netzwerk eingesetzt werden, welches nicht über Active Directory verfügt.

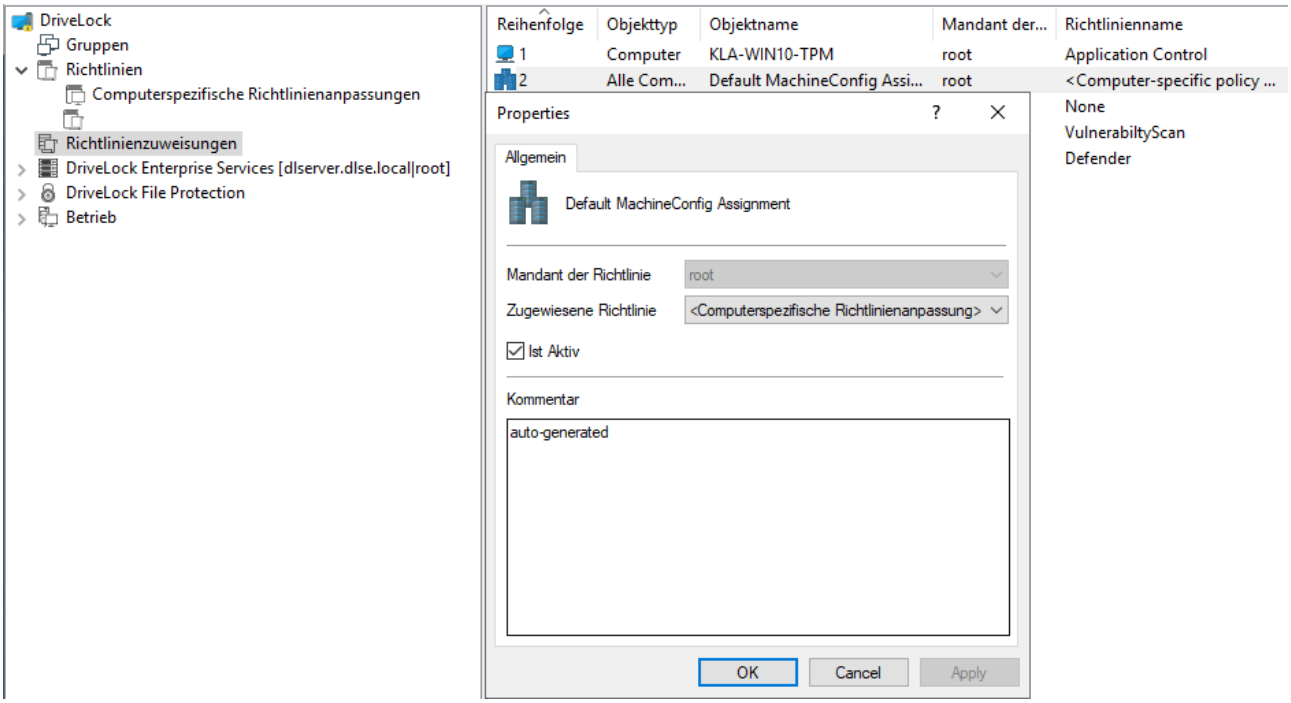
Konfiguration löschen: Mit diesem Befehl löschen Sie eine bestehende DriveLock Konfiguration (lokal oder in Gruppenrichtlinien).

Lokale Computer-Richtlinie in Haupt-Konsole anzeigen: Wählen Sie diese Option, wenn Sie sich die Einstellungen einer lokalen Richtlinie auch als eigenen Knoten im Richtlinien-Editor der DriveLock Management Konsole anzeigen lassen wollen. Dieser Befehl steht u.a. auch auf oberster Ebene in der DMC im Kontextmenü von DriveLock zur Verfügung.



4.2.6 Computerspezifische Richtlinienanpassungen

Eine Computerspezifische Richtlinienanpassung (CRA) ist technisch eine zentral gespeicherte Richtlinie, die nur Einstellungen für einen einzigen Computer enthält. Im Unterschied zu normalen zentral gespeicherte Richtlinie werden diese aber nicht einzeln zugewiesen, sondern über eine einzige Richtlinienzuweisung, deren Zugewiesene Richtlinie die Computerspezifische Richtlinienanpassung ist.



- Standardmäßig wird eine solche Zuweisung unter der Bezeichnung Default MachineConfig Assignment angelegt. Diese Zuweisung liefert für jeden Computer die zu ihm gehörige CRA.
- CRAs werden z.B. für computerspezifische BitLocker-Passworteinstellungen verwendet. Eine CRA wird bei Bedarf automatisch erzeugt.
- CRAs werden von den anderen Richtlinien getrennt in einem eigenen Knoten verwaltet bzw. angezeigt.
- CRAs funktionieren auch, wenn der DriveLock Agent nicht konfiguriert ist, zentral gespeicherte Richtlinien zu verwenden. In diesem Fall benötigt der Agent eine konfigurierte Server-Verbindung.

4.2.7 Richtlinie für permanente Freigaben

Diese Sonderform einer zentral gespeicherten Richtlinie ist dafür vorgesehen, schnell und unkompliziert Laufwerke freigeben oder Anwendungen auf DriveLock Agenten aus dem DriveLock Operations Center (DOC) heraus blockieren zu können. Dazu werden Laufwerks- oder Anwendungsregeln für verschiedene Verhaltensweisen erstellt und im DOC konfiguriert.

In der DriveLock Management Konsole (DMC) wird die Richtlinie für permanente Freigaben im Knoten **Richtlinien** angezeigt.

Eigenschaften

- Die Richtlinie für permanente Freigaben wird automatisch vom Server beim Erstellen der ersten Regel angelegt.
- Jede Änderung an Regeln erzeugt eine neue Version der Richtlinie. Diese wird automatisch veröffentlicht.
- Eine Richtlinienzuweisung wird automatisch vom Server beim Erstellen der Richtlinie für permanente Freigaben angelegt. Sie ist allen Computern zugewiesen, kann aber verändert werden.
- Die Priorität der Zuweisung sollte so eingestellt werden, dass sie höher als die der angewandten Richtlinien ist.
- Eine Richtlinie für permanente Freigaben gilt nur für den jeweiligen Mandanten. Pro Mandant gibt es also nur eine Richtlinie.
- Folgende Berechtigungen können gesetzt werden:
    - Verwalten von Regeln: Anlegen, Ändern und Löschen von Regeln
    - Verwalten von Objekten in Regeln: Hinzufügen bzw. Löschen der verwalteten Objekte in Regeln
    - Lesen von Regeln: Anzeige der Regel

Einschränkungen

- Wir empfehlen, die Regeln nur im DOC zu bearbeiten. Sie können die Richtlinie für permanente Freigaben aber auch aus der DMC heraus öffnen. Bitte beachten Sie hierbei, dass Sie in diesem Fall im DOC keine Änderungen an den Regeln durchführen können.
- Die Regeln können nur von DriveLock Agenten mit einer Version 2020.2 oder höher ausgewertet werden.
- Bei Regeln für Benutzer und Computer ist es sinnvoll, mit Gruppen zu arbeiten
- Das genaue Regelwerk sollte vorbereitet werden, damit Sie im Betrieb effizient Laufwerke oder Anwendungen bestehenden Regeln zuordnen können.

4.3 Richtlinienzuweisung

Im Knoten Richtlinienzuweisungen legen Sie die Zuweisungsreihenfolge und das Zuweisungsziel Ihrer Richtlinien fest. Weitere Informationen finden Sie hier.

4.3.1 RSoP-Planung

Der DriveLock Agent führt alle ihm zugewiesenen Richtlinien in der vorgegebenen Reihenfolge zu einer endgültigen Richtlinie (Richtlinienergebnissatz, RSoP = Resulting Set of

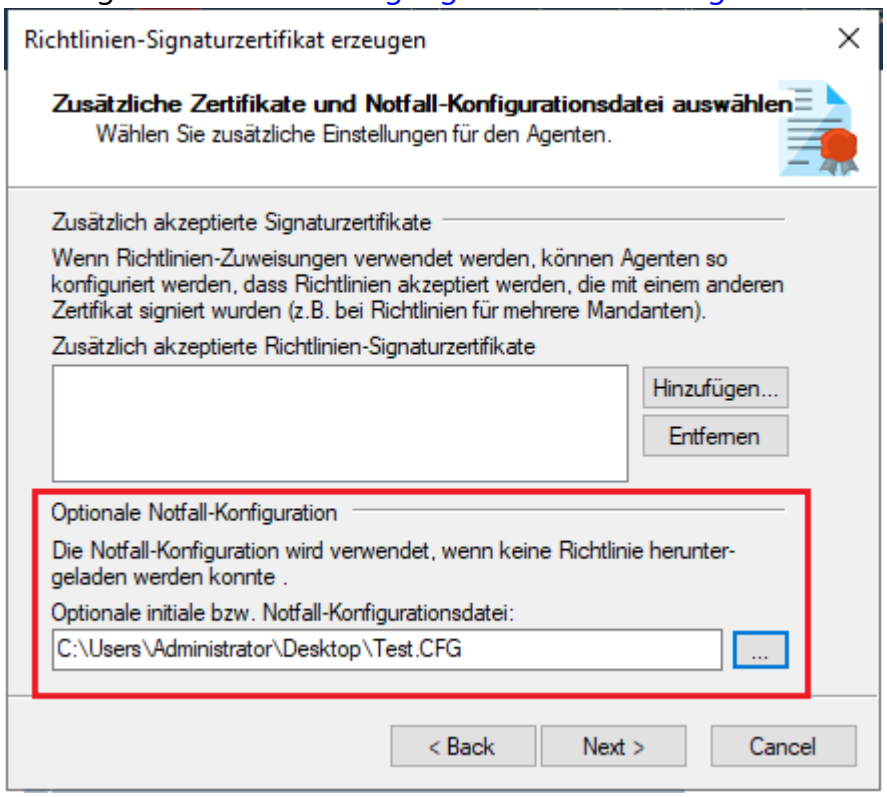
Policies) zusammen.

In der DriveLock Management Konsole (DMC)

Wenn Sie ein RSoP bereits aus der DMC auswerten möchten, öffnen Sie den Knoten **Richtlinienzuweisung**, klicken dann rechts und wählen **RSOP-Planung**. Geben Sie einen Computer aus ihrem AD an, um sich die RSoP anzeigen zu lassen.

Dafür wird je nach Agentenkonfiguration eine der folgenden Kombinationen verwendet (Reihenfolge der Auswertung):

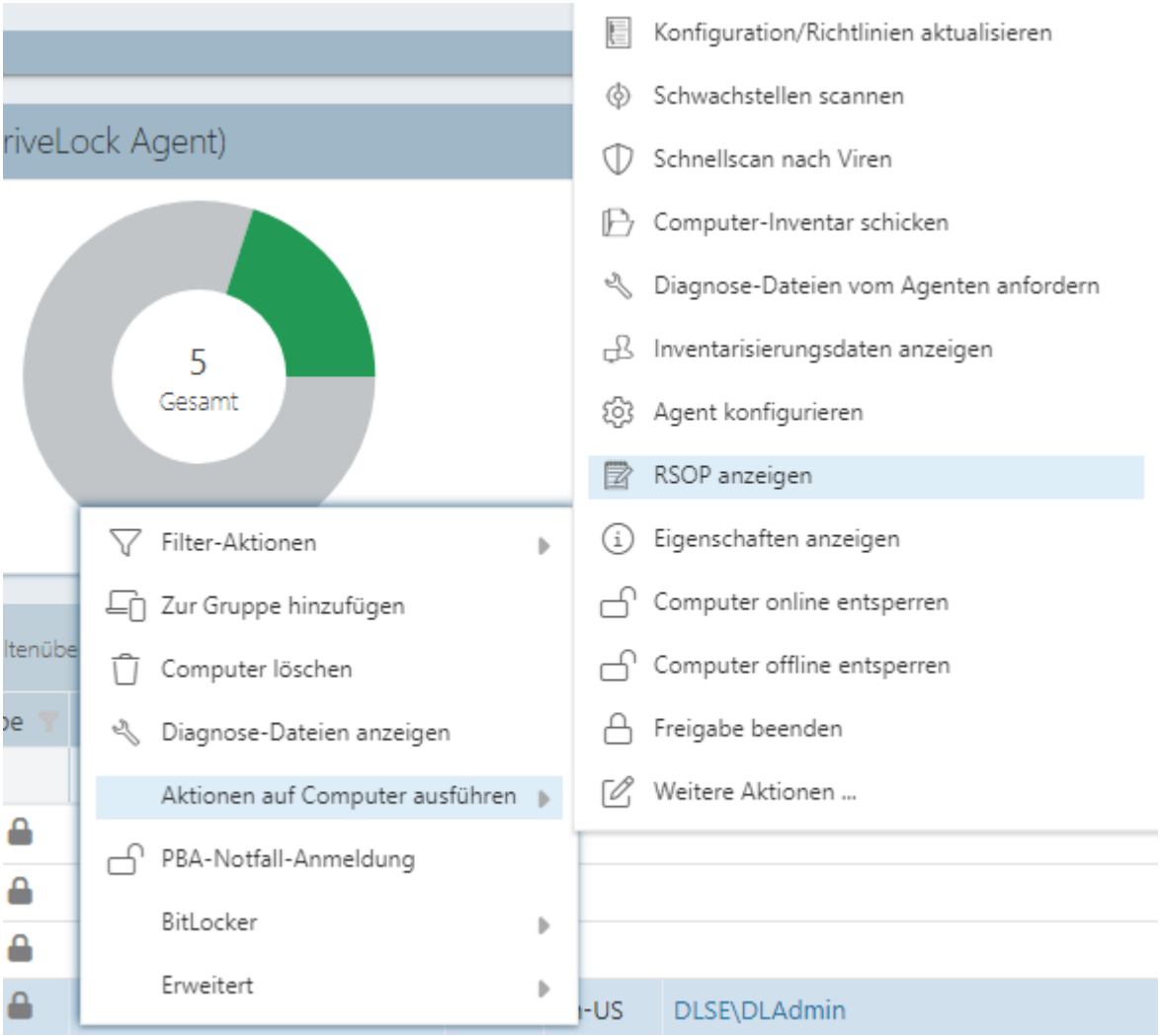
1. Fest eingestellte Richtlinie (Einstellung unter Agentenkonfiguration, Reiter Allgemein, Option Richtlinienzuweisungen ignorieren, feste Richtlinie verwenden) + computerspezifische Richtlinienzuweisung (CRA)
2. Richtlinienzuweisungen
3. Konfigurationsdatei + computerspezifische Richtlinienzuweisung (CRA)
4. Lokale Konfiguration + Gruppenrichtlinienobjekt + computerspezifische Richtlinienzuweisung (CRA)
5. Notfall-Konfigurationsdatei (spezielle Konfigurationsdatei auf einem Agenten), Einstellung während der Erzeugung des Richtlinien-Signaturzertifikats, siehe Abbildung):



Über die Agenten-Fernkontrolle können Sie sich die RSoP anzeigen lassen, um zu sehen, welche Richtlinien der Agent verwendet hat.

Im DriveLock Operations Center (DOC)

Wenn Sie sich ein RSoP aus dem DOC heraus anzeigen lassen wollen, öffnen Sie im Menü **Betrieb** die Ansicht **Computer** und wählen einen Computer aus. Gehen Sie wie in der Abbildung gezeigt vor:



4.4 DriveLock Enterprise Services (DES)

4.4.1 Server

Der DriveLock Enterprise Service ist die zentrale Server-Komponente einer DriveLock Installation. Dabei ist er für die Verarbeitung der Ereignisse verantwortlich, d.h. er nimmt die entstandenen DriveLock-Ereignisse der Agenten entgegen, fügt diese der zentralen Datenbank hinzu und verknüpft die Ereignisse mit verschiedenen Randparametern untereinander. Gleichzeitig dient er allen DriveLock Agenten und der DriveLock Management Konsole als Schnittstelle für Datenbankabfragen und zum Speichern und Laden von wichtigen Dateien (z.B. Wiederherstellungsschlüssel).

Einen Überblick über die DriveLock Komponenten sowie Informationen zur Installation erhalten Sie im DriveLock Installationshandbuch auf DriveLock Online Help.

4.4.1.1 Betriebsmodus des DES

Der DriveLock Enterprise Service kann unterschiedlich betrieben werden:

- als zentraler DriveLock Enterprise Service oder
- als verknüpfter DriveLock Enterprise Service (auch als Linked DES bezeichnet)

Typischerweise werden Sie in Ihrer Systemumgebung nur einen einzigen zentralen DriveLock Enterprise Service installieren. Verknüpfte DriveLock Enterprise Services kommen nur in größeren Systemumgebungen (z.B. mit mehreren Standorten) oder bei der Installation durch einen Security Service Provider (SecaaS) vor.

4.4.1.1.1 Zentraler Server

Der erste DriveLock Enterprise Service einer Infrastruktur ist immer ein zentraler Server, mit direkter Datenbankanbindung. Jeder Weitere ist ein verknüpfter DriveLock Enterprise Service, der nur über den zentralen DriveLock Enterprise Service auf die Datenbank zugreifen kann bzw. an diesen die Ereignisse und Daten weiterleitet.

Da das Verarbeiten der Ereignisse einige Zeit benötigt, wird in diesem Modus zuerst in einen lokalen Cache und anschließend zeitversetzt in die Datenbank geschrieben. Dabei können Lastspitzen besser abgefangen werden. Gleichzeitig wird dadurch sichergestellt, dass es auch in größeren Systemumgebungen (>20.000 Clients) zu keinen Engpässen bei der Verarbeitung von Ereignissen kommt.

Der Cache ist standardmäßig auf 100.000 Ereignisse gesetzt. Ist der Cache voll, werden alle weiteren Ereignisse von Agenten abgelehnt. Der Agent bekommt eine entsprechende Rückmeldung und probiert später erneut, die Ereignisse abzusetzen. Währenddessen schreibt der DriveLock Enterprise Service weiter Ereignisse in die Datenbank.

Im Eigenschaftendialog des Servers können Sie die Cacheeinstellungen auf dem Reiter **Optionen** anpassen.

> Hinweis: Wenn der DriveLock Enterprise Service beendet wird, wird der Cache standardmäßig in die Datei `%PROGRAMDATA%\CenterTools DriveLock\SavedCache.db3` geschrieben.

4.4.1.1.2 Verknüpfter Server

Verknüpfte Server sind besonders geeignet für Standorte mit unzureichenden Internetverbindungen. Sie sind direkt mit dem zentralen DES verbunden und können eine große Anzahl an Ereignissen

- komprimiert und
- bandbreitenschonend nur zu geplanten Zeiten an den DES übertragen.

Außerdem kommt ein verknüpfter DriveLock Enterprise Service zum Einsatz, wenn DriveLock durch einen Security Service Provider installiert und betreut wird.

Folgende Aufgaben können von einem verknüpften Server durchgeführt werden:

- Ereignisse verarbeiten (alle): wird per Schedule an den zentralen DriveLock Enterprise Service weitergeleitet
- Agent-Alive Status senden: wird per Schedule an den zentralen DriveLock Enterprise Service weitergeleitet
- Recovery-Daten hochladen: Daten werden gleich zum zentralen DriveLock Enterprise Service weitergeleitet
- Inventardaten von DriveLock Agenten verarbeiten: werden gleich zum zentralen DriveLock Enterprise Service weitergeleitet
- Installationspakete vom zentralen DriveLock Enterprise Service holen und den Agenten bereitstellen
- Zentral gespeicherte Richtlinien vom zentralen DriveLock Enterprise Service holen und den Agenten bereitstellen
- Active Directory Gruppen- und Benutzerinventardaten zum zentralen DriveLock Enterprise Service hochladen (siehe auch Active Directory Objektinventar eines Mandanten)
- Agenten-Fernverbindungsanfragen vom zentralen DriveLock Enterprise Service entgegennehmen und an den richtigen Agenten weiterleiten (Agent-Remote Proxy)

Hinweis: Die Verarbeitung von Inventar-Daten von Agenten mit einer älteren DriveLock Version ist nicht möglich.

Auf dem Reiter **Allgemein** im Eigenschaftendialog des verknüpften DES können Sie festlegen, wie oft der Upload vom verknüpften zum zentralen DriveLock Enterprise Service erfolgen soll. Standardmäßig erfolgt der Upload jede Stunde.

Auf dem Reiter **Optionen** unter Anzahl der Ereignisse pro Hochladevorgang (verknüpfter Server) geben Sie an, wie viele Ereignisse am verknüpften DriveLock Enterprise Service zwischengespeichert werden sollen, bis der Upload zum zentralen DriveLock Enterprise Service erfolgt. Ist dieser Wert zu hoch, dauert es ggf. sehr lange bis Ereignisse am zentralen DriveLock Enterprise Service ankommen und somit im Reporting sichtbar sind. D.h., handelt es sich nur um eine kleine Außenstelle, an der täglich max. 10.000 Ereignis anfallen und man aber täglich ein Reporting machen möchte, muss dieser Wert von 20.000 z.B. auf 10.000 oder gar 5.000 eingestellt werden.

Hinweis: Nach Erreichen der definierten Cachegröße wird dieser standardmäßig komprimiert in das Verzeichnis `%PROGRAMDATA%\CenterTools DriveLock\Storage` geschrieben.

Hinweis: Der zentrale, empfangende DriveLock Enterprise Service speichert den Cache standardmäßig in das Verzeichnis `%PROGRAMDATA%\CenterTools DriveLock\ReceivedStorage`.

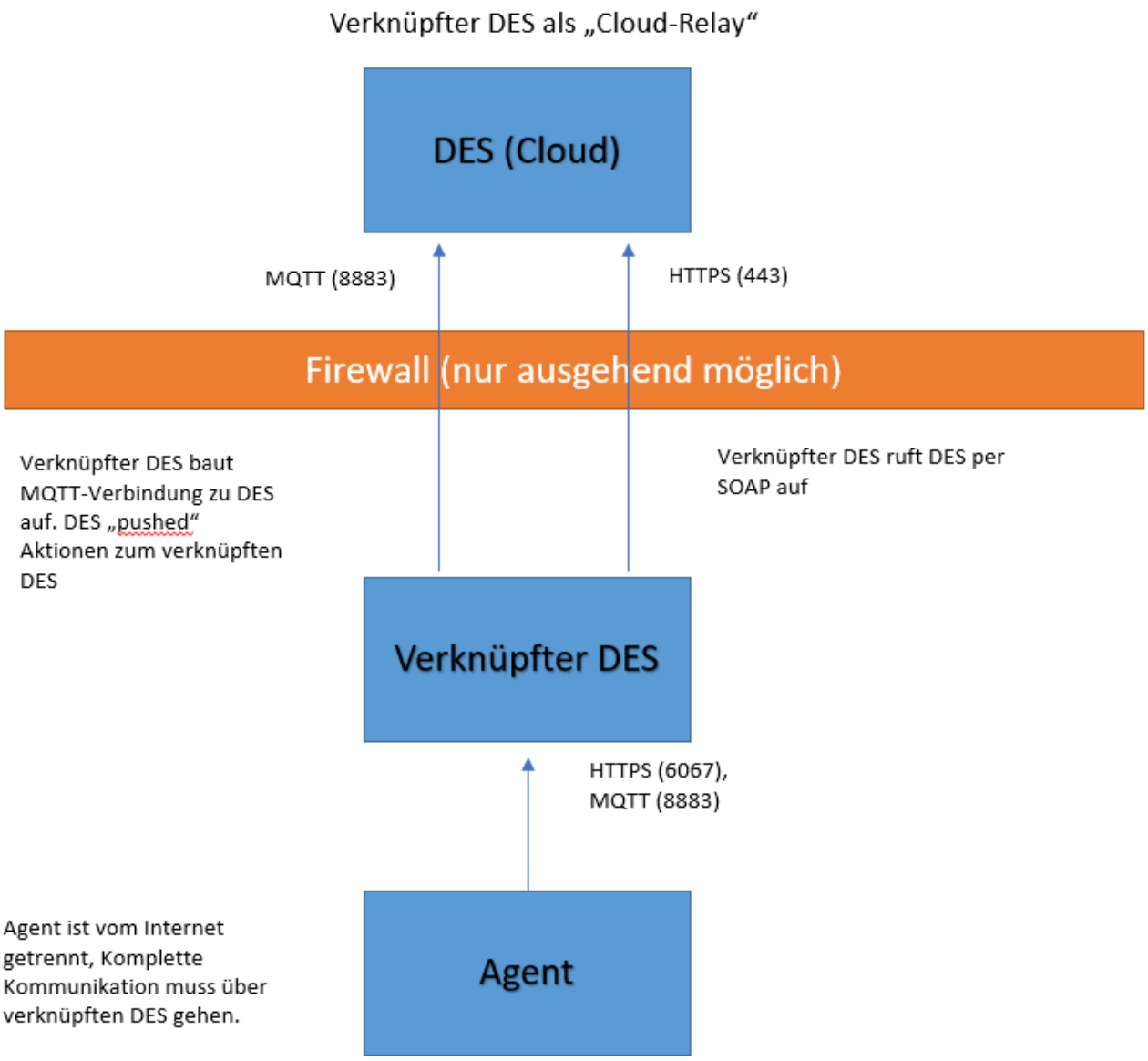
4.4.1.1.2.1 Verknüpfter DES zur Anbindung an die DriveLock Cloud

Der verknüpfte DES im Cloud-Modus dient als Vermittler, um Agenten ohne Internetverbindung mit der DriveLock Cloud zu verbinden.

Dabei erfüllt er drei Aufgaben:

1. Weiterleiten von Anfragen der Agenten an die Cloud
2. Caching von Daten des zentralen DES
3. Bereitstellen eines MQTT Brokers
    - Ermöglicht es, Agenten per Agentenfernkontrolle zu kontrollieren
    - Erlaubt dem zentralen DES in der Cloud, den verknüpften DES zu erreichen

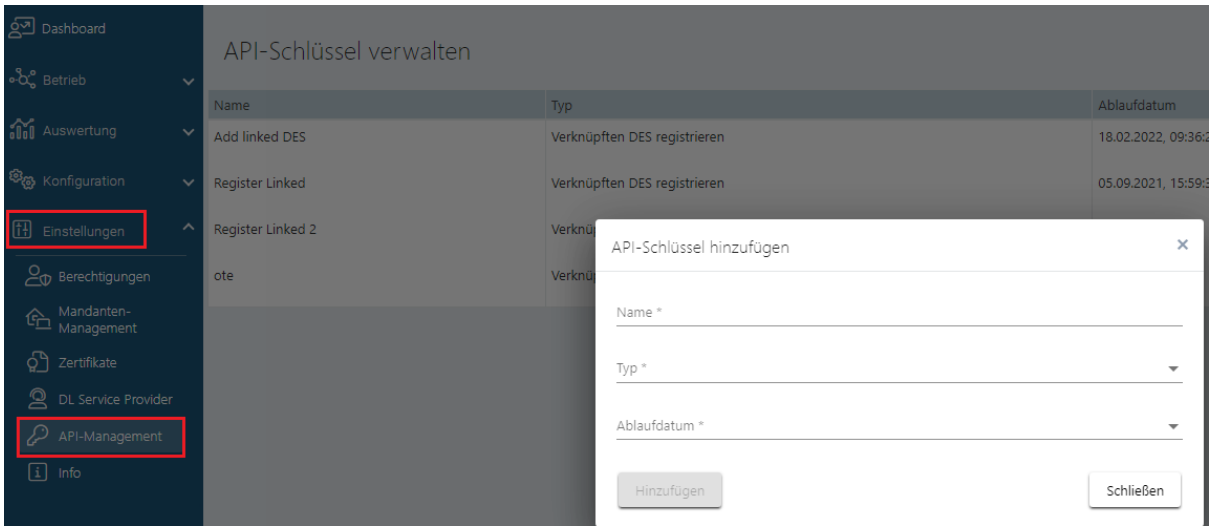
Netzwerkdiagramm:



4.4.1.1.2.2 Verknüpften DES als Cloud-Relay registrieren

Gehen Sie folgendermaßen vor, um einen verknüpften DES zu registrieren:

1. Erzeugen Sie einen API-Schlüssel, der die Registrierung des verknüpften DES im Cloud-Mandanten erlaubt.
2. Dazu öffnen Sie im DOC die Ansicht **Einstellungen**und dann **API-Management**, siehe Abbildung:



3. Legen Sie einen neuen Schlüssel vom Typ **Verknüpften DES registrieren** an.
4. Das Ergebnis ist eine lange Zeichenfolge (API-Schlüssel), der zur Autorisierung dient. Der Schlüssel muss jetzt auf einem sicheren Weg auf den verknüpften DES übertragen werden. Welche Methode Sie wählen, ist Ihnen überlassen.

> Hinweis: Beachten Sie, dass der Schlüssel ein Ablaufdatum hat. Dies bedeutet nur dass Sie mit dem Schlüssel bei Erreichen des Ablaufdatums keine verknüpfte DES mehr mit der Cloud registrieren können, jedoch nicht, dass der verknüpfte DES dann nicht mehr funktioniert. Nach Verwendung können Schlüssel also auch ohne Bedenken gelöscht werden.

5. Registrieren Sie den verknüpften DES in der Cloud im Datenbank-Installationsassistenten.
6. Öffnen Sie hierzu den Datenbank-Installationsassistenten und wählen Sie dort die Option **Verknüpfter DriveLock Enterprise Service zur Anbindung an die DriveLock Cloud**.

7. Kopieren Sie im nächsten Dialog den API Schlüssel ins Textfeld.
8. Klicken Sie **Server registrieren**.

4.4.1.1.3 Betriebsmodus nach der Installation ändern

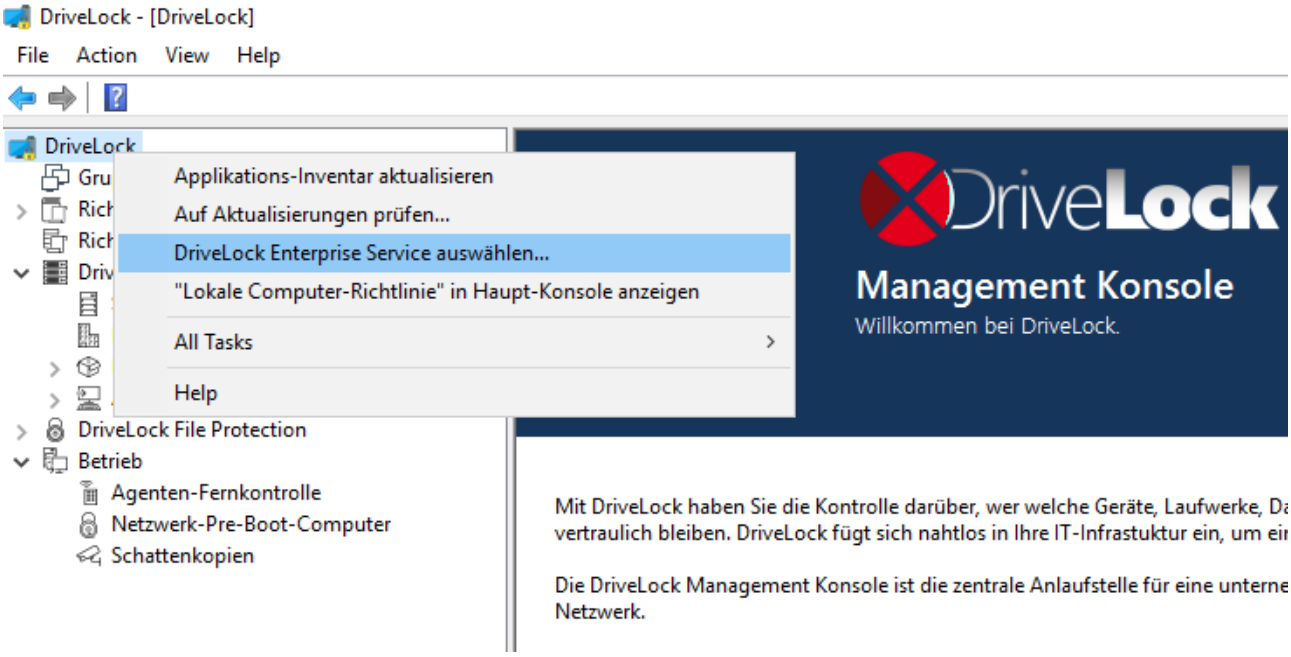
Der Betriebsmodus wird unmittelbar nach der Installation des DriveLock Enterprise Service durch den Datenbank-Installationsassistenten eingerichtet. Wenn Sie nach der Installation den Betriebsmodus ändern wollen, muss dieser Assistent erneut geöffnet werden:

Wählen Sie hier beispielsweise die zweite Option **Verknüpfter DriveLock Enterprise Service**. Weitere Informationen zu Installation des DriveLock Enterprise Service finden Sie im DriveLock Installationshandbuch auf DriveLock Online Help.

4.4.1.2 Verbindung zum DES auswählen

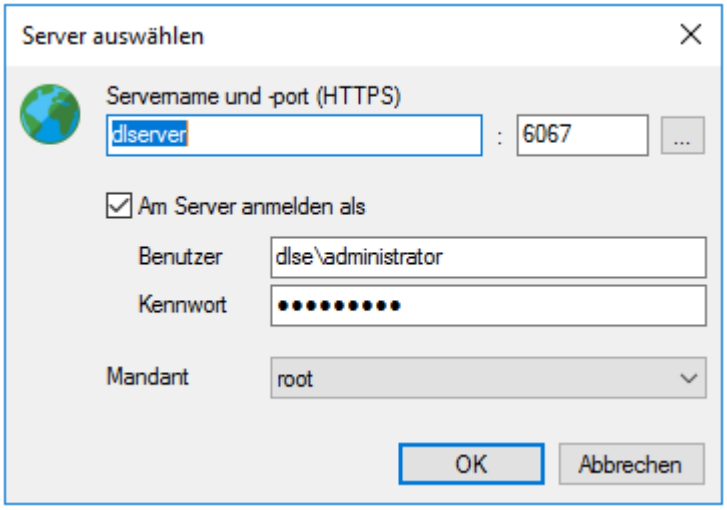
Die DriveLock Management Konsole verbindet sich an verschiedenen Stellen mit dem DriveLock Enterprise Service, um dort Informationen zu speichern (z.B. Lizenzdaten oder zentral gespeicherte Richtlinien) oder Daten vom DriveLock Enterprise Service abzufragen. Daher muss zunächst auch für die DriveLock Management Konsole eine Verbindung zum DriveLock Enterprise Service konfiguriert werden.

Entweder rechtsklicken Sie auf **DriveLock** und wählen **DriveLock Enterprise Service auswählen...** aus dem Kontextmenü.



Oder Sie klicken auf **DriveLock Enterprise Services**und wählen dort aus dem Kontextmenü **DriveLock Enterprise Service auswählen...**.

Als nächstes geben Sie den Servernamen, Mandanten und Ihre Verbindungsdaten ein.



Hinweis: Wenn sich die DriveLock Management Konsole zum ersten Mal mit dem DES verbindet, wird das DES Zertifikat geprüft. Weitere Informationen finden Sie im Kapitel Zertifikate.

Konnte die DriveLock Management Konsole beim ersten Start über DNS-SD bereits den DriveLock Enterprise Service ermitteln, ist dieser bereits eingetragen. Ansonsten geben Sie hier den gewünschten Servernamen ein. Sofern Sie bei der Installation des DriveLock Enterprise Service den Standard-Port geändert haben, müssen Sie auch hier den neuen Port eintragen.

Soll der Zugriff nicht über Ihr aktuelles Benutzerkonto erfolgen, haben Sie die Möglichkeit hier ein anderes Benutzerkonto mit Passwort einzutragen, das die DriveLock Management Konsole für die Verbindung zum DriveLock Enterprise Service verwendet.

Achtung: Achtung: Das für die Verbindung zum DriveLock Enterprise Service verwendete Benutzerkonto muss auch die entsprechenden Berechtigungen erhalten haben. Ein berechtigtes Konto / eine berechtigte Gruppe kann entweder bei der Installation des DriveLock Enterprise Service angegeben werden (siehe DriveLock Installationshandbuch), oder es wird über die DriveLock Enterprise Service Einstellungen nachträglich eingerichtet.

Zusätzlich können Sie auswählen, zu welchen Mandantendaten diese Verbindung führen soll (nur wichtig, sofern sie eine DriveLock Umgebung für mehrere Mandanten betreiben).

4.4.1.2.1 Verbindungseinstellungen für Proxy-Server

Die DriveLock Management Konsole verwendet Systemproxy-Einstellungen. Für manche Aktionen kann ein expliziter Proxy angegeben werden. Weitere Informationen finden Sie hier.

4.4.1.2.1.1 Proxy-Einstellungen auf dem DriveLock Agenten

Sie können die Einstellungen für den Proxy-Server auch direkt auf dem Agenten setzen. Dazu dienen die beiden Kommandozeilenbefehle:

- `drivelock -setproxy <proxytype>;<proxy>`
  - `<proxytype>` spezifiziert den Proxytyp und kann named, pac, none oder netsh sein
  - `<proxy>` enthält entweder den Proxy oder die URL für die Proxy Auto-Konfigurationsdatei

- `drivelock -setproxyaccount <auth-scheme>;<proxyuser>;>proxypassword>`

Beispiele für die Verwendung:

```
drivelock -setproxy name;myproxy:myport

drivelock -setproxy pac;//myhttpserver/myproxy.pac

drivelock -setproxy none

drivelock -setproxy netsh
```

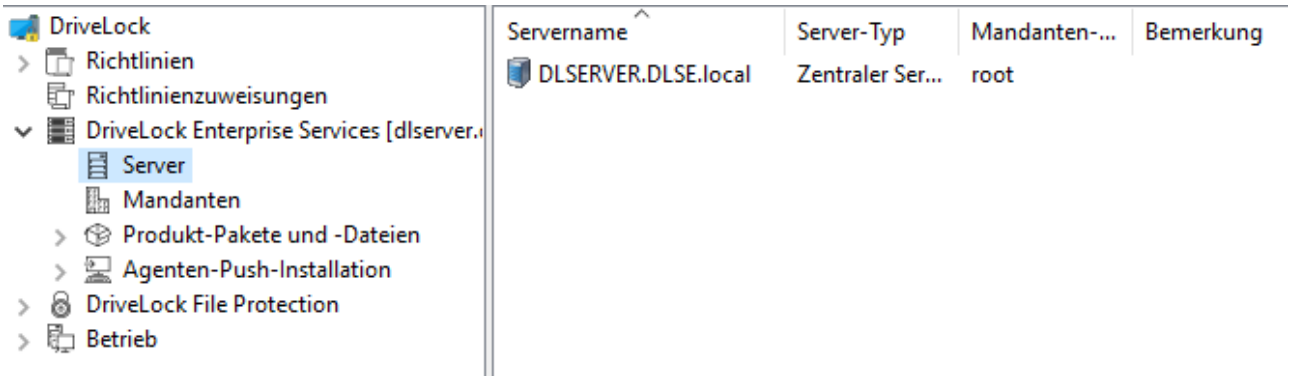
Wenn der Proxy eine Authentifizierung benötigt, können Sie den Benutzer und das Kennwort mit dem Befehl `drivelock -setproxyaccount <auth-scheme>;<proxyuser>;>proxypassword>` setzen. Dabei wird mit `<authscheme>` das Authentifizierungsschema (`basic, ntlm, passport, digest und negotiate`) angegeben.

Diese Einstellungen werden in der Registry unterhalb des Registry-Schlüssels `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DriveLock\Parameters` gespeichert. Sie werden vorrangig ausgewertet, d.h. wenn ein Proxy mit dem Befehl `drivelock -setproxy` gesetzt wurden, werden alle anderen Einstellungen ignoriert.

> Achtung: Proxy-Einstellungen, die bei der Ausführung des MSI (siehe Installationshandbuch) angegeben oder mit dem Befehl `drivelock -setproxy` gesetzt wurden, können mit `drivelock -removeproxy` gelöscht werden.

4.4.1.3 Einstellungen für den DES

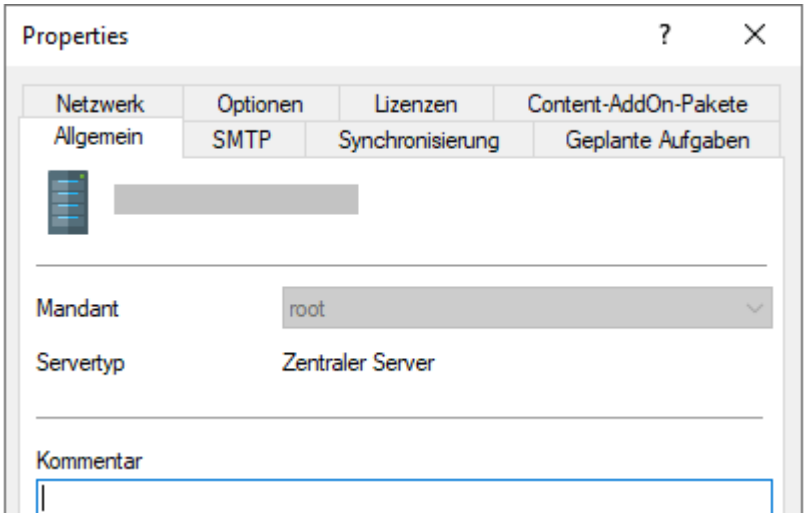
Unter **Server** werden alle DriveLock Enterprise Services angezeigt, die sich registriert haben:



In der Spalte **Server-Typ** wird der jeweilige Betriebsmodus eines jeden Servers angezeigt. Pro Server und je nach Betriebsmodus können verschiedene Einstellungen im Eigenschaftendialog getroffen werden.

> Hinweis: Hier werden die Einstellungen pro DriveLock Enterprise Service verwaltet. Der Name des DriveLock Enterprise Service entspricht dem Computernamen des Servers.

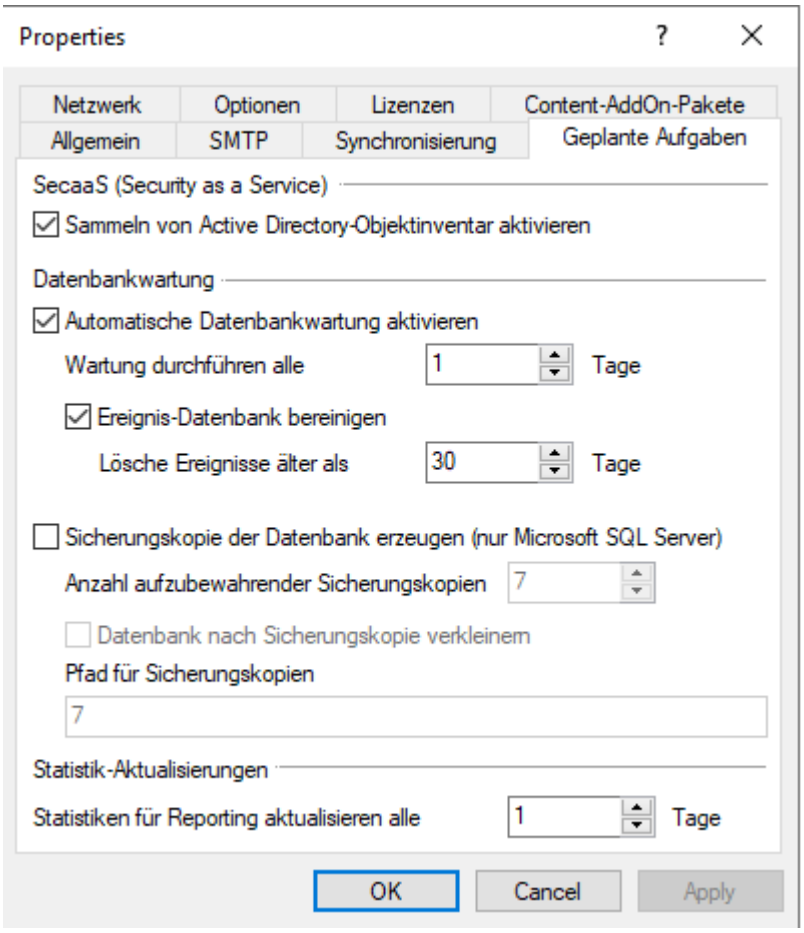
Durch einen Doppelklick auf den Servernamen öffnen Sie den Eigenschaftendialog. Informationen zu den einzelnen Reitern finden Sie im Folgenden.

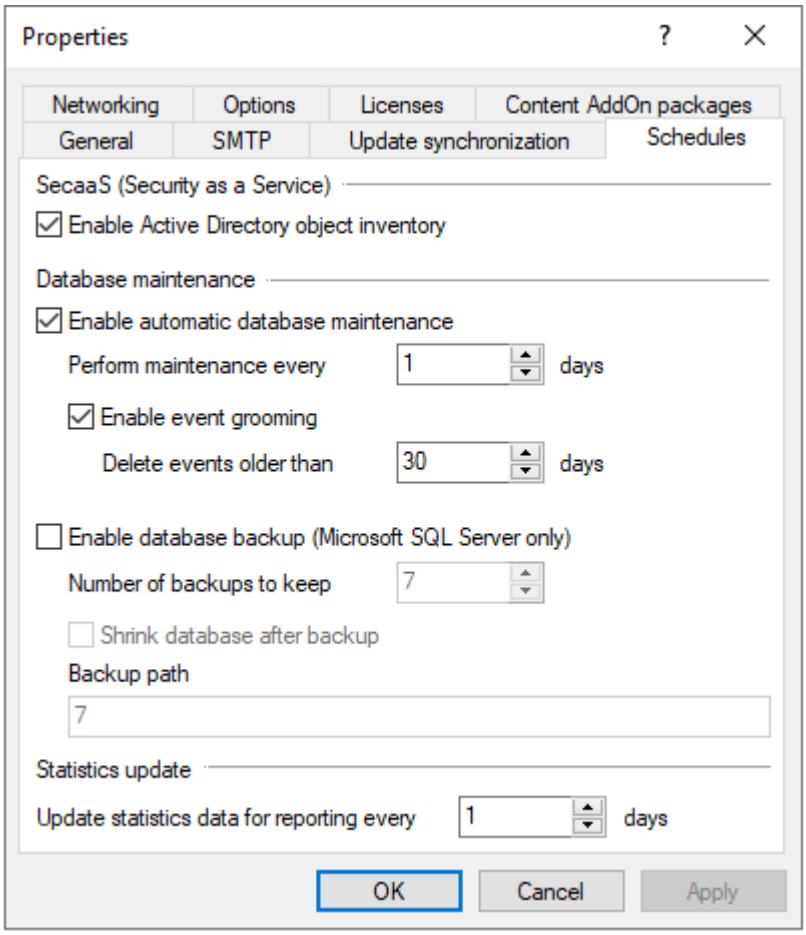


4.4.1.3.1 Geplante Aufgaben

Die Datenbankwartung dient zur Einschränkung des Datenwachstums und zur Pflege der Indexe auf den Tabellenspalten, um bestmögliche Performance auch bei großen Datenmengen zu gewährleisten.

> Hinweis: Die Optionen zur Datenbankwartung sollten im DriveLock Enterprise Service nur dann konfiguriert werden, wenn ein SQL Server Express Version verwendet wird (z.B. MSDE 2000, SQL2005 Express, SQL2008 Express). Für die Vollversion des SQL-Server wird empfohlen, die Datenbankwartung manuell auf dem Server einzustellen. Weitere Informationen hierzu erhalten Sie von unserem Support oder im Database Guide unter Technical Articles auf DriveLock Online Help.


Properties
Netzwerk
Optionen
Lizenzen
Content-AddOn-Pakete
Allgemein
SMTP
Synchronisierung
Geplante Aufgaben
SecaaS (Security as a Service)
Sammeln von Active Directory-Objektinventar aktivieren
Datenbankwartung
Automatische Datenbankwartung aktivieren
Wartung durchführen alle
1
Tage
Ereignis-Datenbank bereinigen
Lösche Ereignisse älter als
30
Tage
Sicherungskopie der Datenbank erzeugen (nur Microsoft SQL Server)
Anzahl aufzubewahrender Sicherungskopien
7
Datenbank nach Sicherungskopie verkleinern
Pfad für Sicherungskopien
7
Statistik-Aktualisierungen
Statistiken für Reporting aktualisieren alle
1
Tage
OK
Cancel
Apply



Um das Wachstum der SQL-Datenbank einzuschränken, kann der DriveLock Enterprise Service automatisch alte Ereignisse löschen. Sie sollten die Datenbankbereinigung einstellen, wenn Sie keine Reports oder forensischen Analysen anhand von alten Daten erstellen müssen, oder wenn Sie Ihre SQL-Daten mit einem Drittanbieter-Tool archivieren.

Um die Datenbankbereinigung zu aktivieren, klicken Sie auf **Automatische Datenbankwartung aktivieren** und wählen das maximale Alter der Ereignisse. Diese Option muss deaktiviert werden, wenn Sie manuell einen Wartungsjob am SQL-Server eingerichtet haben.

Standardmäßig werden alle Ereignisse, die älter als 30 Tage sind, täglich automatisch gelöscht.

Die Wartung der Indexe auf den Tabellenspalten wird ebenfalls über die Option **Automatische Datenbankwartung aktivieren** eingeschaltet. Dadurch wird die Suche optimiert. Diese Option muss deaktiviert werden, wenn Sie manuell einen Wartungsjob am SQL-Server eingerichtet haben.

Standardmäßig wird die Datenbankpflege täglich automatisch durchgeführt.

Die Option **Sammeln von Active Directory-Objektinventar aktivieren** wird hier beschrieben.

4.4.1.3.1.1 Sammeln von Active Directory-Objektinventar

Jeder DriveLock Enterprise Service ist in der Lage, aus dem aktuellen Active Directory (d.h. der gleichen Domäne, der auch das Servicekonto des DriveLock Enterprise Service-Dienst Benutzerkontos angehört) alle Benutzer, Computer, Gruppen und OU-Informationen als AD-Objektinventar auszulesen und in der DriveLock Datenbank für die Verwendung innerhalb einer DriveLock Konfiguration abzuspeichern.

Nutzen Sie diese Möglichkeit vor allem dann, wenn Sie eine DriveLock Konfiguration für DriveLock Agenten mit Berechtigungen für Benutzer oder Gruppen aus einer anderen Domäne erstellen möchten.

Wird die DriveLock Management Konsole von einem Rechner aus gestartet, der in der gleichen Domäne liegt, für die auch die Konfiguration erstellt wird, ist es nicht notwendig die Benutzer und Gruppen aus dem Active Directory auszulesen, da die DriveLock Management Konsole direkt auf diese Daten zugreifen kann. Allerdings kann auch in diesem Fall das AD-Objektinventar zur Konfiguration verwendet werden und insbesondere in größeren AD-Umgebungen zu einem Performance-Vorteil gegenüber dem direkten Zu-griff führen.

Damit ein DriveLock Enterprise Service ein Active Directory Objektinventar erzeugt, muss diese Option zunächst in den Einstellungen des DriveLock Enterprise Service aktiviert werden.

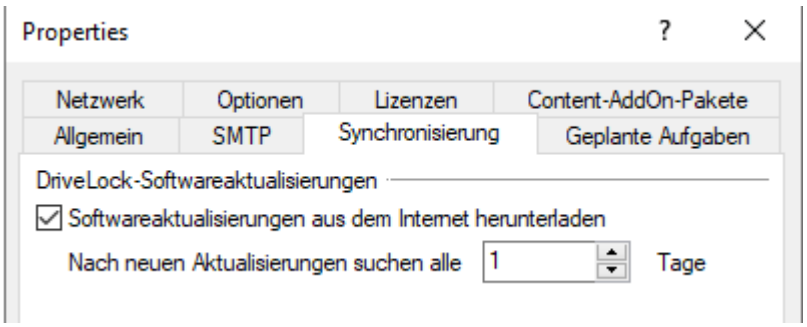
Da die Option **Sammeln von Active Directory-Objektinventar aktivieren** standardmäßig aktiviert ist, ermittelt der DriveLock Enterprise Service automatisch einmal alle 24 Stunden alle Benutzer und Gruppen der aktuellen Domäne und gleicht diese mit der in seiner Datenbank gespeicherten Daten ab (Synchronisierung). Auch hier werden die Daten nach Mandanten getrennt gespeichert, sofern Sie mehrere Mandanten angelegt haben.

Sobald ein AD-Objektinventar vorhanden ist, kann dieses bei der Konfiguration innerhalb der DriveLock Management Konsole verwendet werden.

Hier können Sie nun die Option zum automatischen Laden des AD-Objektinventars aktivieren. Soll dieser Vor-gang einmal am Tag automatisch erfolgen, aktivieren Sie auch hier die entsprechende Option. Zusätzlich wird der Zeitpunkt des letzten erfolgten Ladevorgangs angezeigt.

4.4.1.3.2 Synchronisierung

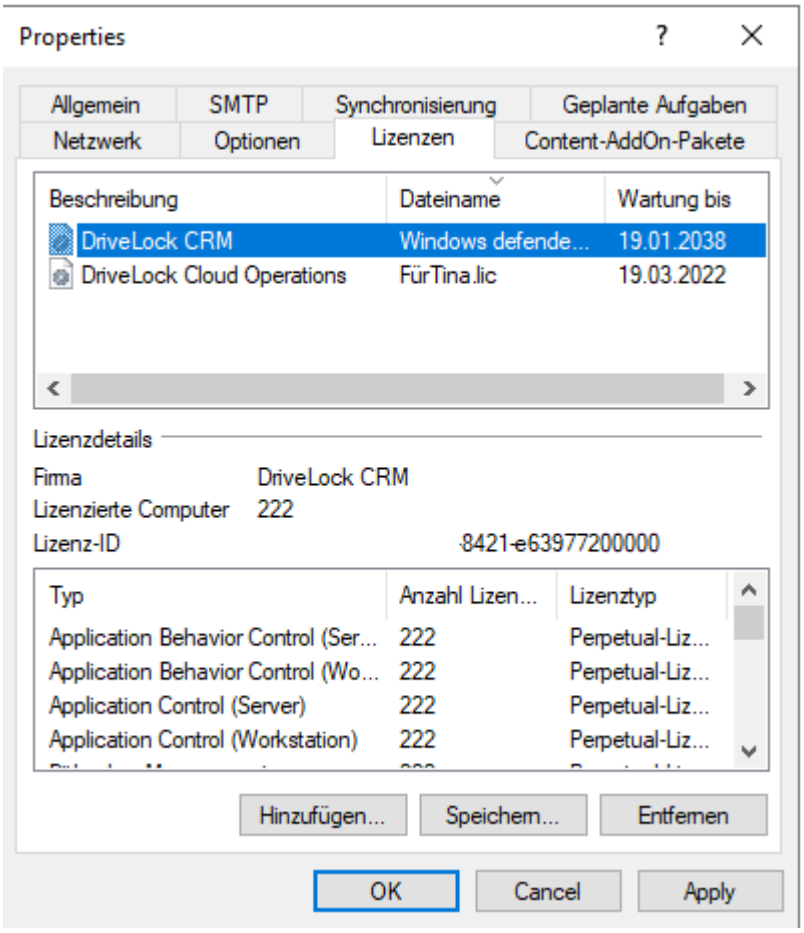
Mit Hilfe der Synchronisierungseinstellungen legen Sie fest, ob und wie oft der DriveLock Enterprise Service über eine Internetverbindung nach neuen DriveLock Softwarepaketen sucht.



4.4.1.3.3 Lizenzen

Wenn Sie eine neue DriveLock Konfiguration anlegen und eine Lizenzdatei einlesen, können Sie diese zum DriveLock Enterprise Service übertragen. Dadurch werden für verschiedene Bereiche (z.B. Security Awareness Content AddOn, Festplattenverschlüsselung) zusätzliche Funktionen beim DriveLock Enterprise Service aktiviert.

Im Eigenschaften-Fenster des DriveLock Enterprise Service können Sie die gespeicherten Lizenzen anzeigen und nicht mehr benötigte Lizenzen löschen. Wählen Sie dazu den Reiter **Lizenzen**:



Sobald Sie im oberen Bereich eine Lizenz auswählen, werden die Lizenzdetails im unteren Bereich angezeigt.

Markieren Sie eine Lizenz und klicken Sie auf Entfernen, um die markierte Lizenz aus der DriveLock Datenbank zu löschen.

4.4.1.3.4 Netzwerk

Netzwerkeinstellungen können für den zentralen DES sowie für verknüpfte DriveLock Enterprise Services vorgenommen werden. Sie können auf dem Reiter **Netzwerk** eingesehen und geändert werden.

Eine der grundlegenden DriveLock Enterprise Service Einstellungen ist der Port, auf dem der Dienst hört und Daten bzw. Abfragen entgegennimmt.

> Hinweis: Beachten Sie, dass die Angabe des Ports auch an anderen Stellen in der DMC gesetzt werden kann. Außerdem wird das Zertifikat für den DES auch an den Port gebunden.

Die **Externe URL** bezieht sich auf die Adresse, die z.B. bei Push-Installation dem Client als Serveradresse mitgegeben wird. Diese sollte der Server-Adresse in den Richtlinien entsprechen.

Die Übertragung der Ereignisse zwischen DriveLock Agent und DriveLock Enterprise Service erfolgt standardmäßig verschlüsselt. Aus diesem Grund ist die Option **HTTPS erzwingen** standardmäßig gesetzt.

Um die Konfiguration einheitlich zu halten, sollte diese Einstellung für alle DriveLock Enterprise Services auf den gleichen Wert gesetzt werden.

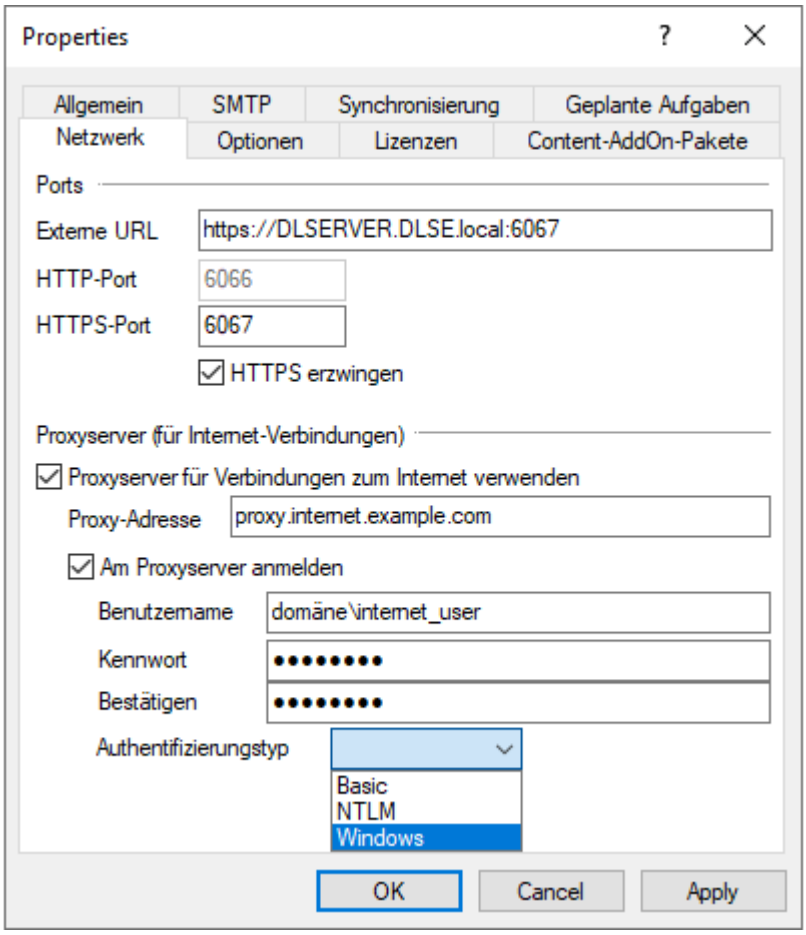
> Achtung: Wenn die Standard-Ports geändert werden, muss dies in der DriveLock Richtlinie für die Agenten ebenfalls geändert werden, unter: Erweiterte Konfiguration – Globale Einstellungen – Server-Verbindungen.

Weiter zu den Proxyserver-Einstellungen.

4.4.1.3.4.1 Proxyserver verwenden

Für das automatische Update und für die automatische Aktualisierung der Antiviren-Definitionen wird eine Internetverbindung benötigt. Falls der Zugriff ins Internet nur über einen Proxyserver möglich ist, muss dieser pro DriveLock Enterprise Service eingestellt werden.

Folgende Optionen sind möglich:



- **Proxyserver für Verbindungen zum Internet verwenden**: Der dort angegebene Proxyserver wird verwendet um auf das Internet zuzugreifen. Ggf. ist die Angabe eines Ports nötig, der durch „:“ getrennt angegeben wird, z.B.: proxy.internal.example.com:8080
- **Am Proxyserver anmelden**: Muss nur angegeben werden, falls kein anonymer Zugriff über den Proxy möglich ist.
- **Benutzername**: Ein Benutzer, der über den Proxy ins Internet darf. Ggf. muss die Domäne mit angegeben werden, z.B.: domäne\internet_user
- **Kennwort**: Das zum Benutzer passende Kennwort.
- **Authentifizierungstyp**: Es werden verschiedene Authentifizierungstypen angeboten, um sich gegen den Proxyserver zu authentifizieren. Die dort ausgewählte Variante muss vom Proxyserver unterstützt werden:
    - **Basic**: Die Übermittlung von Benutzer und Passwort erfolgt im Klartext
    - **NTLM**: Es wird der dort angegebene Benutzer für den Internetzugriff verwendet. Das Passwort wird verschlüsselt übertragen.

- **Windows**: Windows integrierte Anmeldung, es wird das Dienstkonto vom DriveLock Enterprise Service für den Internetzugriff verwendet (und nicht der im Dialog angegebene Benutzer).

4.4.1.3.5 SMTP

Die E-Mail-Server Einstellungen werden für den Versand von Reports verwendet. Dazu wird in dem Feld **SMTP-Server** der entsprechende Server angegeben. Der Standard-Port ist 25.

Falls der SMTP-Server eine Anmeldung erfordert, um interne Emails zu versenden, können unter Benutzername und Kennwort die Daten hierfür angegeben werden.

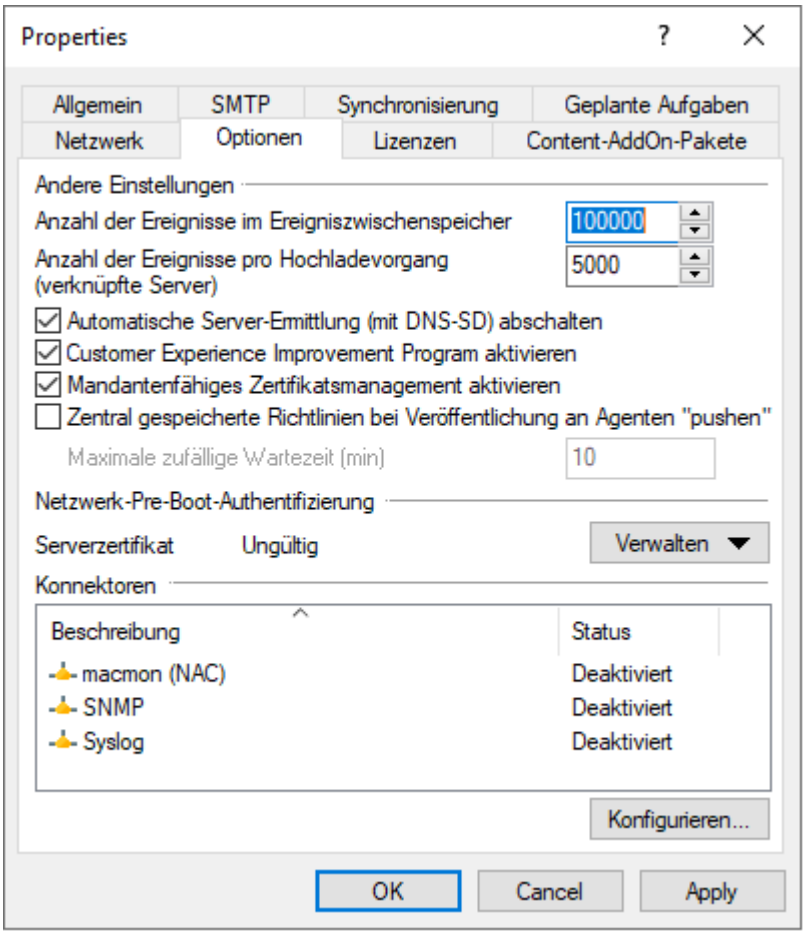
Weiter können Sie den Absender-Namen der Email und die Absender Email-Adresse angeben. Unter Email-Adresse muss i.d.R. eine interne Email-Adresse verwendet werden.

4.4.1.3.6 Content-AddOn-Pakete

Hier legen Sie fest, ob und wie oft der DriveLock Enterprise Service über eine Internetverbindung nach neuen Security Awareness Content Addon Paketen sucht.

4.4.1.3.7 Optionen

Wir empfehlen, auf dem Reiter **Optionen** generell die vorgegebenen Standardeinstellungen zu übernehmen.

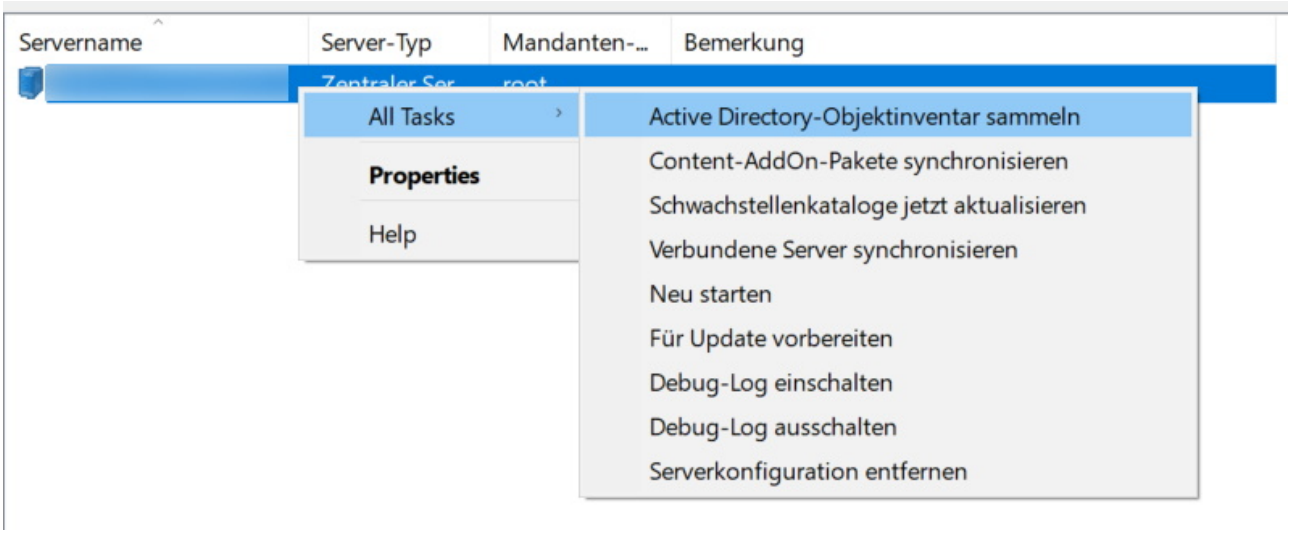


Optionen im Detail:

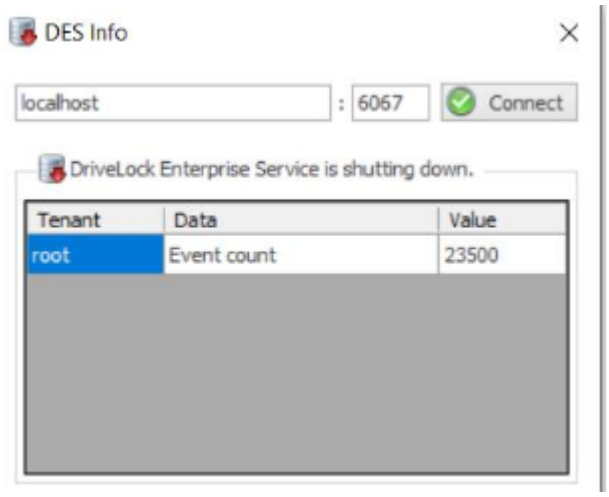
- Wenn Sie **Customer Experience Improvement Program aktivieren**, werden statistische Daten zur Geschwindigkeit und Häufigkeit genutzter Funktionen gesammelt, anonymisiert und zu DriveLock hochgeladen. Dies hilft, das Produkt weiter zu verbessern. Persönliche bzw. personenbezogene Daten werden nicht gespeichert oder übertragen. Wenn Sie nicht an dem Programm teilnehmen möchten und keine Daten zu DriveLock hochgeladen werden sollen, können Sie die Option deaktivieren.
- Agenten aktualisieren ihre Richtlinien standardmäßig alle 30 Minuten. Durch das Aktivieren der Option **Zentral gespeicherte Richtlinie bei Veröffentlichung an Agenten "pushen"** wird eine schnellere Aktualisierung der Richtlinie am Agenten durchgeführt.

4.4.1.4 Manuelle Aktionen am DES starten

Öffnen Sie das Kontextmenü des DES und wählen Sie **Alle Aufgaben** (All Tasks). Hier haben Sie folgende Optionen, um manuelle Aktionen durchzuführen:



1. **Active Directory-Objektinventar sammeln**: Der DriveLock Enterprise Service ermittelt automatisch einmal alle 24 Stunden alle Benutzer und Gruppen der aktuellen Domäne und gleicht diese mit der in seiner Datenbank gespeicherten Daten ab (Synchronisierung).
2. **Content-AddOn-Pakete synchronisieren**: Wenn Sie Security Awareness verwenden, können Sie mit diesem Befehl die Daten über erworbene AddOn-Pakete aktualisieren und dann auf den DES herunterladen. Weitere Informationen finden Sie in der Security Awareness Dokumentation auf DriveLock Online Help.
3. **Schwachstellenkataloge jetzt aktualisieren**: Wenn Sie den DriveLock Vulnerability Scanner einsetzen, können Sie mit diesem Befehl die Schwachstellenkataloge aktualisieren lassen. Weitere Informationen finden Sie in der Vulnerability Scanner Dokumentation auf DriveLock Online Help.
4. **Verbundene Server synchronisieren**: Wählen Sie diesen Befehl, wenn Sie diverse Daten (Richtlinien, Security-Awareness-Pakete uns Agenten-Installationspakete) auf allen verknüpften DES zum zentralen DES synchronisieren wollen.
5. **Neu starten**: Der DES wird neu gestartet. Wenn Sie verknüpfte DES einsetzen, können Sie diese ohne direkten Zugriff neu starten.
6. **Für Update vorbereiten**: Der DES unterbricht die Kommunikation mit den DriveLock Agenten und nimmt keine weiteren Daten an. Zuerst werden die Ereignisse verarbeitet und der DES wird gestoppt und wieder gestartet. Wir empfehlen diese Vorgehensweise in großen Umgebungen. Über das Taskleistensymbol erhalten Sie eine Übersicht:



7. **Debug-Log ein**- bzw. **ausschalten**: Aktivieren bzw. deaktivieren Sie mit diesem Befehl detaillierte Debug-Informationen in den Protokolldateien. Die Änderung ist sofort aktiv und erfordert keinen Neustart des Dienstes.
8. **Serverkonfiguration entfernen**: Mit diesem Befehl wird die komplette Serverkonfiguration gelöscht. Dies ist z.B. sinnvoll, wenn Sie nicht genutzte Server entfernen wollen.

4.4.1.5 Status des DES

Anhand des DES Taskleistensymbols können Sie die Erreichbarkeit des DriveLock Enterprise Services überwachen und überprüfen. Ist der Dienst nicht erreichbar, wird dies rot argestellt. Während des Dienststarts kann es ein paar Minuten dauern, bis der Status auf grün wechselt.

Durch einen Doppelklick auf das Icon öffnet sich die Detailansicht.

Hier werden verschiedene Verbindungsinformationen angezeigt, wie die Adresse, Datenbankserver, Datenbanktyp, Datenbankname oder deren Version.

Durch einen Rechtsklick auf das Icon erscheint ein Kontextmenü, über das Sie schnell einen Neustart des DriveLock Enterprise Service oder für den Support hilfreiche Aktionen durchführen können.

4.4.2 Mandanten

DriveLock und der DriveLock Enterprise Service unterstützen die Verwendung von mehreren Mandanten. Ein Mandant ist eine separate, komplett getrennte Datenbank. In dieser Datenbank werden alle Daten, die zu diesem Mandanten gehören, gespeichert. Diese logische und physische Trennung versteht man als Mandantenfähigkeit. Ein DriveLock Agent kann jeweils mit einem Mandanten verknüpft werden.

Folgendes Prinzip liegt dahinter: Ein zentraler DriveLock Enterprise Service wird vom Systemhaus betrieben, der mehrere kleine Kundeninstallationen betreut. Bei jedem Kunden ist ein verknüpfter DriveLock Enterprise Service installiert und mit dem zentralen DriveLock Enterprise Service des Systemhauses verbunden. Für jede Kundeninstallation wird ein eigener Mandant betrieben. Dadurch werden die Daten getrennt und mit unterschiedlichen Zugriffsrechten versehen, damit ein Kunde nicht die Berichte eines anderen Kunden sehen kann.

Damit Ereignisse zu einem Mandanten zugeordnet werden können, kann pro Mandant ein dedizierter verknüpfter DriveLock Enterprise Service eingerichtet werden:

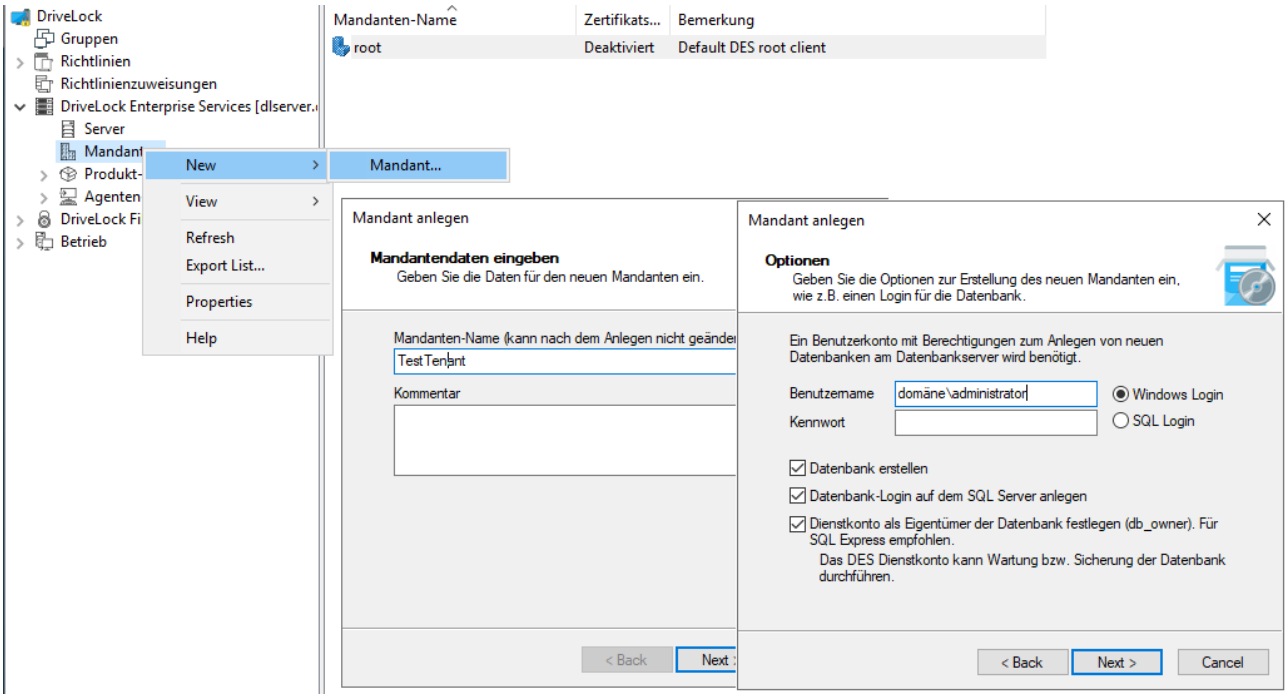
- Server1 (zentraler DES, Standardmandant „root“)
- Server2 (verknüpfter DES zu Server1, Standardmandant „B“)
- DriveLock Agenten (Serververbindung zu Server2, Mandant „B“)

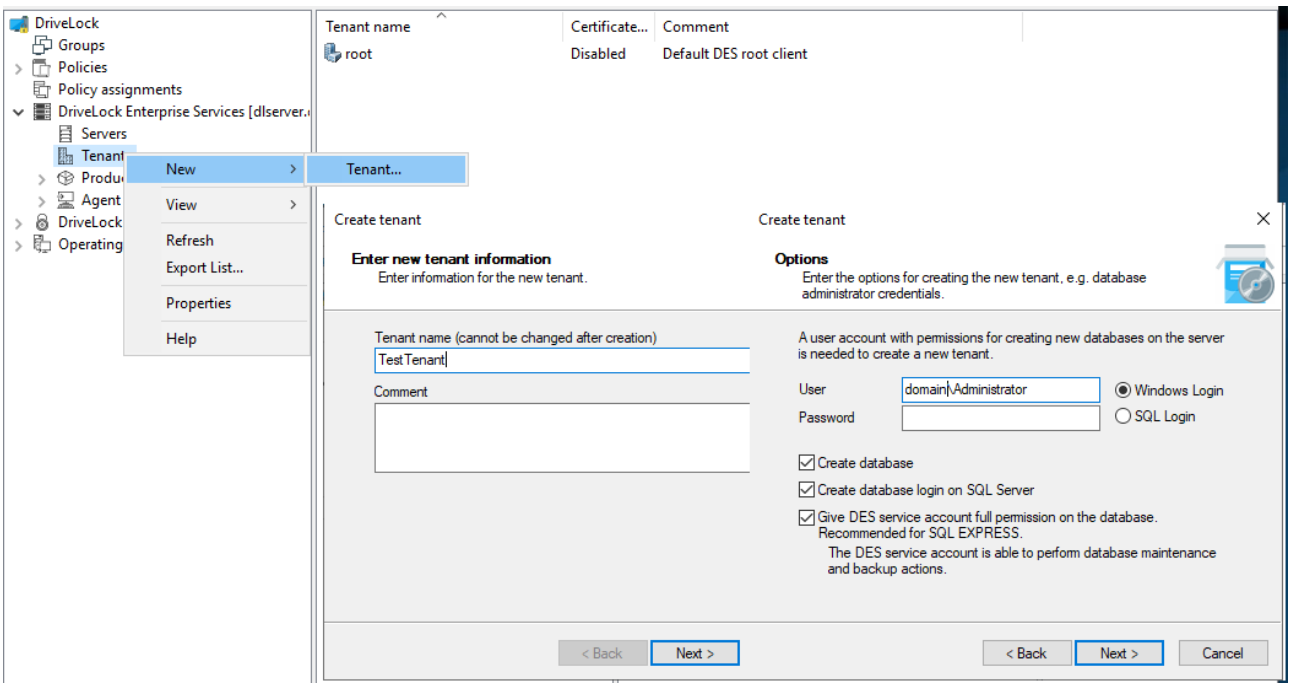
Der Standardmandant eines Server kann über die DriveLock Management Konsole – DriveLock Enterprise Services – Server – <Auswahl des Servers> - Rechtsklick Eigenschaften – Mandant zugeordnet werden.

4.4.2.1 Mandant anlegen oder löschen

Der Standardmandant root wird automatisch angelegt, sobald Sie die Installation des DES und der Datenbanken abgeschlossen haben.

Um einen weitere Mandanten anzulegen, rechts-klicken Sie unter DriveLock Enterprise Services auf Mandanten und wählen Neu und dann Mandant.





Geben Sie einen Namen für den neuen Mandanten an. Es dürfen keine Sonderzeichen oder Umlaute enthalten sein. Die maximale Länge des Namens ist auf 50 Zeichen begrenzt.

Ähnlich wie bei der Installation der DriveLock Datenbank können hier entsprechende Einstellungen für die Installation getroffen werden.

Nun wählen Sie aus den vorhandenen Benutzern bzw. Gruppen, welche bereits für den Zugriff auf den DriveLock Enterprise Service konfiguriert wurden, diejenigen aus, die Lese-

zugriff auf die innerhalb der DriveLock Management Konsole verfügbaren Mandantendaten haben sollen.

Am Datenbankserver selbst wird nun die neue Datenbank angelegt.

> Hinweis: Wenn Sie mit dem Anlegen des Mandanten fertig sind, wird eine neue Datenbank <Stammname>_<Mandanten-Name> angelegt, wobei der <Stammname> der Datenbankname ist, der bei der Installation des DriveLock Enterprise Service angegeben wurde. In der Voreinstellung ist dies DRIVELOCK.

Mandant löschen

Um einen Mandanten und die verknüpfte Datenbank zu löschen, rechts-klicken Sie unter DriveLock Enterprise Services – Mandanten, wählen den zu löschenden Mandanten aus, und klicken dann **Mandant löschen**.

> Hinweis: Die Datenbank des Mandanten wird dabei nicht gelöscht und sollte manuell entfernt werden.

4.4.2.2 DriveLock Agenten einem Mandanten zuordnen

Standardmäßig wird ein DriveLock Agent dem Standardmandanten **root** zugeordnet. Soll ein anderer Mandant verwendet werden, müssen Sie dies bei der Installation angeben. Weitere Informationen finden Sie im Installationshandbuch auf DriveLock Online Help.

Die Zuordnung eines Agenten zu einem Mandanten kann auch nachträglich über die Agenten-Fernkontrolle oder über Kommandozeilenbefehle geändert werden.

4.4.3 Produkt-Pakete und -Dateien

4.4.3.1 Produktaktualisierung

In der DriveLock Management Konsole hat man unter dem Knoten **DriveLock Enterprise Services**, **Produkt-Pakete und -Dateien** im Unterknoten **Softwarepakete** Zugriff auf die lokal verwalteten und online verfügbaren DriveLock Installationspakete.

Die Aktualisierung der DriveLock Komponenten wird am DES verwaltet. Der DES kann bei bestehender Internetverbindung die DriveLock Pakete herunterladen. Alternativ können in offline Umgebungen die Pakete manuell eingespielt werden.

Die Pakete mit Bezugsquelle Cloud sind von DriveLock veröffentlicht worden und können in die lokale Verwaltung aufgenommen werden. Auf neue Pakete werden sie über eine Benach-

richtigung beim Start der MMC aufmerksam gemacht. Pakete mit Bezugsquelle DES sind lokal verfügbar und können verwaltet / freigegeben werden.

Über einen Rechtsklick – Herunterladen kann man das Installationspaket für die weitere Verwendung lokal speichern oder über Eigenschaften sich weitere Details dazu anzeigen lassen.

> Hinweis: Für einen möglichst reibungslosen Updateverlauf sollten die Server und Management-Komponenten zuerst und erst danach die Agenten aktualisiert werden.

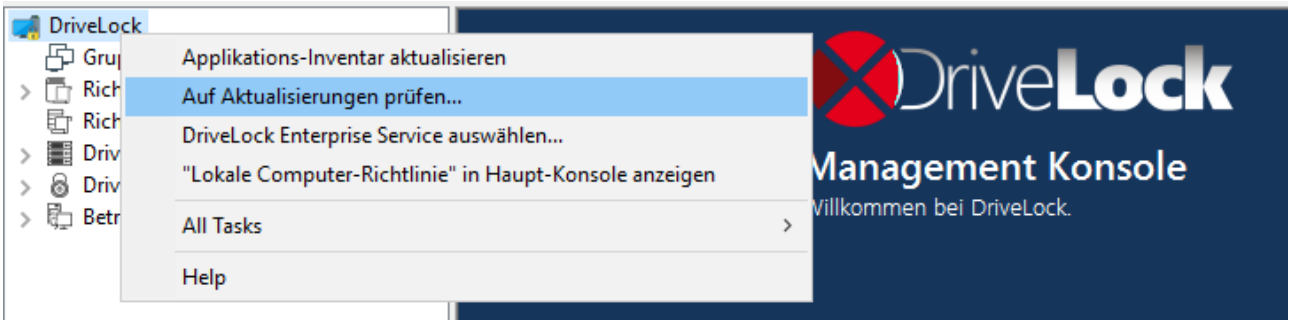
Mit dem Kontextmenu **Auf den DES downloaden** auf ein Paket, welches die Bezugsquelle **Cloud** hat, können sie neue Pakete in die Verwaltung mit aufnehmen.

Über das Kontextmenu auf den Menüpunkt **Softwarepakete** können sie die Pakete aus der Cloud ein/ausblenden und manuell Pakete zum DES hochladen und diese in die Verwaltung aufnehmen. Dies ist z.B. bei offline-Systemen erforderlich.

Jedes Paket ist mit einem Freigabe- bzw. Veröffentlichungsstatus versehen, so dass eine Aktualisierung nur von neueren Paketversionen gemacht wird, die auch freigegeben bzw. veröffentlicht sind.

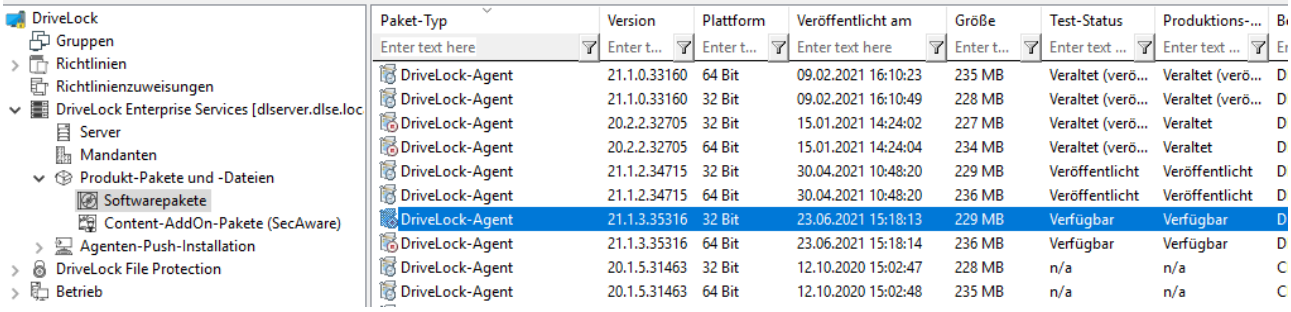
4.4.3.2 Auf neue Versionen prüfen

Rechts-klicken Sie auf **DriveLock** und wählen Sie **Auf Aktualisierungen prüfen...**.



Die Anwendung verbindet sich nun mit der DriveLock Webseite und prüft, ob eine neue Version vorhanden ist. Falls ja, werden eine entsprechende Meldung und Informationen zur neuen Version angezeigt. Sie können hier auch angeben, wie oft automatisch nach Aktualisierungen geprüft werden soll.

Eine weitere Möglichkeit, um die neueste veröffentlichte Version zu überprüfen, finden Sie im Navigationsbereich im Knoten **DriveLock Enterprise Services** unter **Produkt-Pakete und -Dateien** im Unterknoten **Softwarepakete**:



Hier sehen Sie die aktuellsten zur Zeit verfügbaren Installationspakete von DriveLock und können diese über das Kontextmenü eines Eintrages sofort und einzeln herunterladen.

Ebenso können Sie hier im Unterknoten **Content-AddOn-Pakete (SecAware)** die aktuell freigegebenen Security Awareness Pakete einsehen, die über den DriveLock Enterprise Service (DES) heruntergeladen werden können. Sofern Sie über eine Lizenzierung des Security Awareness Content AddOn verfügen, werden Ihnen alle Module angezeigt, ansonsten sehen Sie alle Module die Sie zu Demo-Zwecken verwenden können. Weitere Informationen finden Sie in der Security Awareness Dokumentation auf DriveLock Online Help.

4.4.3.3 Test- und Produktionsumgebung

Alle DriveLock Agenten sind standardmäßig der Produktionsumgebung zugeordnet. Einzelne Agenten können zu einer Testumgebung ('Staging') zugeordnet werden, um neue Produktversionen getrennt von der Produktionsumgebung aktualisieren und testen zu können.

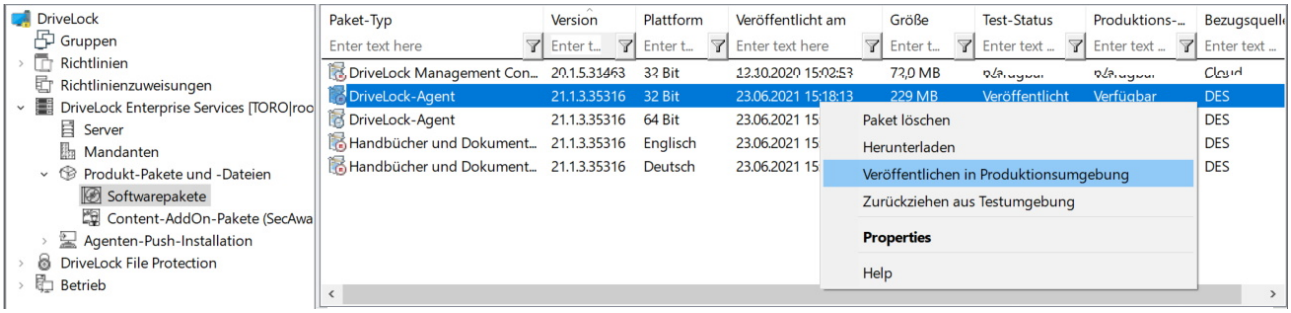
In der Übersicht der Softwarepakete können die Pakete für die Test und/oder Produktionsumgebung freigegeben werden.

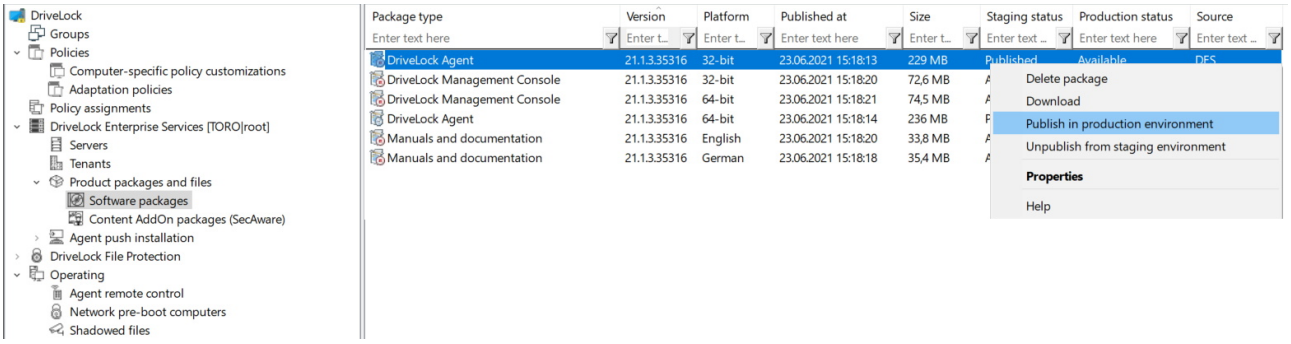
Die Konfiguration der Umgebung (Test bzw. Produktion) für den Agenten kann über folgende Methoden erfolgen:

- Option bei der Agenten-Fernkontrolle
- Zuordnung zur Produktions- / Testumgebung über Kommandozeile direkt am Agenten
- `drivelock.exe -setstaging`: Ordnet den Client der Testumgebung zu
- `drivelock.exe -setproduction`: Ordnet den Client der Produktionsumgebung zu (Standard)

Durch den Freigabestatus beeinflusst man die zu verteilende / installierende Version von DriveLock.

Eine Freigabe wird nur einmal übergreifend für alle DriveLock Enterprise Services vorgenommen. Die Freigabe wird dabei pro Produkt / Version / Plattform vorgenommen.





Es gibt folgende Freigaben:

- Veröffentlicht: Pakete mit diesem Status werden von Clients heruntergeladen und aktualisiert.
- Heruntergeladen: Pakete mit diesem Status sind am DriveLock Enterprise Service vorhanden und werden nicht von Clients heruntergeladen.
- Veraltet (veröffentlicht): Pakete mit diesem Status sind überholt und werden von Clients nur herunterge-laden und aktualisiert, wenn das neuere Paket nicht veröffentlicht ist.
- Veraltet (heruntergeladen): Pakete mit diesem Status sind überholt und sind am DriveLock Enterprise Service vorhanden, werden nicht von Clients heruntergeladen.

Per Rechtsklick auf ein Paket kann eine der folgenden Aktionen gestartet oder eine Freigabe erteilt bzw. zurückgenommen werden:

- Software-Paket löschen: Das ausgewählte Paket wird vom DriveLock Enterprise Service gelöscht. Setzt voraus, dass das Paket nicht für eine Umgebung veröffentlicht ist.
- Heruntergeladen: Das Paket steht am DriveLock Enterprise Service zur Verfügung und wartet auf Ge-nehmigungFreigabe in die Test und/oder Produktionsumgebung.

- Veröffentlichen in Testumgebung / Produktionsumgebung: Erteilt die Freigabe zur Installation in der je-weiligen selektierten Umgebung.
- Zurücknehmen von Testumgebung / Produktionsumgebung: Nimmt die Freigabe zur Installation für die jeweilig selektierte Umgebung zurück.

4.4.4 Agenten-Push-Installation

Die Push-Installation von DriveLock ermöglicht es, den DriveLock Agenten manuell oder automatisch auf den Client-Computern der Endbenutzer (Zielcomputer) zu installieren.

Für die Push-Installation überprüft der DriveLock Enterprise Server regelmäßig, dass alle Computer aus den konfigurierten AD-Gruppen / OUs einen DriveLock Agenten installiert haben. Für Computer ohne DriveLock Installation kann der Administrator im DriveLock Operations Center DOC / Konfiguration / Installation diese Computer auswählen und die Installation manuell starten.

Bei der automatischen Push-Installation können Sie die Installation des DriveLock Agenten für konfigurierte AD Gruppen und OUs konfigurieren. Der DES ermittelt aus dem AD die zugehörigen Computer und stößt die Push-Installation für Computer, die noch kein DriveLock haben, an.

Die manuelle Push-Installation kann vom Administrator aus dem DOC für einzelne Computer auch unabhängig von AD-Gruppen / OUs angestoßen werden.

Für die Push-Installation wird über einen administrativen Zugang der DriveLock Update Service (DlUpdSvc) auf den PC kopiert, installiert und gestartet. Der DlUpdSvc holt sich dann über den DES das aktuell freigegebene Installationspaket und führt die Agenten-Installation durch.

> Hinweis: Die Push-Installation startet nur, wenn in den Softwarepaketen sowohl eine 32-bit als auch ein 64-bit Version des DriveLock-Agenten für die Test- und Produktionsumgebung freigegeben ist.

4.4.4.1 Voraussetzungen für die Push-Installation

Folgende Bedingungen müssen alle erfüllt sein, damit die Push-Installation funktioniert:

- Die Agenten-Installationspakete für 32- und 64-Bit-Betriebssysteme müssen auf dem DES vorhanden sein und in der richtigen Umgebung (Produktion/Test) veröffentlicht werden
- Der Zielrechner muss im Netzwerk erreichbar sein, das DNS muss funktionieren.

- Die Freigabe admin$ des Zielcomputers muss erreichbar sein.
- Auf dem Zielcomputer muss die Datei- und Druckfreigabe aktiviert sein.
- Das Konto, das für die Push-Installation verwendet wird, muss über Administratorrechte auf dem Zielcomputer verfügen.

Hinweis: Die Push Installation funktioniert nur, wenn auch der Server, auf dem der DES installiert ist, die richtige SMB Version unterstützt. Diese kann bei aktuellen Windows Server Versionen nicht aktiviert sein und muss bei Bedarf nachinstalliert werden.

4.4.4.2 Globale Einstellungen pro Server

Die globalen Einstellungen für die Push-Installation werden für jeden DES unabhängig konfiguriert. Damit können die Einstellungen für verschiedene Organisationen eines Unternehmens einfach separiert werden.

Folgende Einstellungen sind auf dem Reiter Allgemein möglich:

- **Synchronisierung mit Active Directory aktivieren**: wenn markiert, ermittelt der DES über die konfigurierten AD-Gruppen die zugehörigen Computer. Im DOC können Computer ohne DriveLock Agent selektiert und installiert werden.
- **Automatische Push-Softwareverteilung aktivieren**: wenn markiert, werden gefundene Computer ohne DriveLock Agent automatisch installiert.

Standard Einstellungen werden sowohl für die automatische Push-Installation als auch für als Voreinstellungen für die Ausführung der Push-Installation im DOC verwendet.

- **Benutzer für die Installation**: der Benutzer muss auf dem lokalen PC administrative Rechte haben.
- **In Testumgebung installieren**: wenn aktiv werden die zu installierenden Computer der Testumgebung zugeordnet.
- **Neustart nach Installation erzwingen**: wenn aktiv werden ohne Rückfrage nach der Installation des Agenten die Computer neu gestartet.
- **Konfigurationstyp**: hier wählen sie aus, mit welcher Art von Richtlinie und welcher Richtlinie die Computer konfiguriert werden.

4.4.4.3 Automatische Push-Gruppen / OUs

In diesem Unterknoten wählen Sie die Computergruppen oder OUs aus dem AD aus, für die Sie die automatisierte oder automatische Push-Installation verwenden möchten.

Klicken Sie rechts auf den Unterknoten, wählen Sie **Neu** und dann **Gruppe...** oder **Organisationseinheit...**, je nachdem, was Sie anlegen wollen.

4.4.4.4 Push-Installation ausführen

Sie können eine neue (manuelle) Push-Installation im DriveLock Operations Center (DOC) im Menü **Konfiguration** unter **Installationen** auf dem Reiter **Installation des Agenten** starten.

Computerauswahl: Hier können Sie mehrere Computer für die manuelle Push-Installation angeben.

Optionen: Hier werden die aktuell für die Push-Installation verwendeten Agenten Installationspakete und ihre Versio-nen für die Test und Produktionsumgebung angezeigt. Dies wird in der MMC unter MMC / DriveLock Enterprise Service / Produkt-Pakete und -Dateien / Softwarepakete verwaltet.

Als weitere Optionen können Sie folgendes angeben:

Benutzerkonto für die Installation verwenden: der Benutzer muss auf dem lokalen PC administrative Rechte haben.

Neustart nach Installation erzwingen: wenn aktiv wird ohne Rückfrage nach der Installation des Agenten der PC neu gestartet.

Installierte DriveLock Agenten entfernen: die Reparatureinstellungen sollen, ggf. nach Rücksprache mit dem DriveLock Support, nur verwendet werden, wenn eine vorhergehende DriveLock Installation fehlgeschlagen ist und eine normale Deinstallation des Agenten nicht mehr möglich ist.

Agentenkonfiguration: Hier kann ein Proxy konfiguriert werden, der vom Update-Service für den Download des Installations-paketes vom DES verwendet wird. Dieser wird auch für die Agenten-Konfiguration übernommen.

Konfigurationsart: hier wählen sie aus, mit welcher Art von Richtlinie und welcher Richtlinie die Computer konfiguriert werden.

4.4.4.5 Automatisches Update

Das automatische Update muss auch für den DriveLock Agenten in einer Richtlinie konfiguriert werden.

Öffnen Sie in Ihrer Richtlinie unter **Globale Einstellungen** den Unterknoten **Einstellungen** und hier **Automatische Aktualisierung**.

4.5 Betrieb

4.5.1 Agenten-Fernkontrolle

DriveLock erlaubt es Ihnen, sich auf einen entfernten Computer zu verbinden, auf dem bereits der DriveLock Agent installiert ist und läuft. Das kann z.B. dafür verwendet werden, um temporär Zugriff auf eine Laufwerksklasse auf einem entfernten Computer zu erlauben oder um den aktuellen Status Ihrer Agenten zu kontrollieren. Es ist beispielsweise auch möglich, sich die zuvor eingesammelten Inventarisierungsdaten anzeigen zu lassen oder eine Hard- und Softwareinventarisierung manuell zu starten.

DriveLock benutzt standardmäßig das HTTPS-Protokoll, um sich auf entfernte Computer zu verbinden. Um eine Verbindung mit einem entfernten Computer aufzunehmen, muss DriveLock auf dem entfernten Computer installiert sein. Um eine Verbindung zu einem Computer aufzubauen, müssen eingehende Verbindungen vom TCP Port 6065 und das Programm „DriveLock“ in den Firewall Einstellungen erlaubt sein. Das HTTP-Protokoll mit dem Port 6064 ist nicht zu empfehlen.

Mithilfe der Schnellkonfiguration über DNS-SD, listet die MMC unter der Agenten-Fernkontrolle alle benachbarten DriveLock Agenten auf. Standardmäßig werden alle DriveLock Agenten aber direkt vom DriveLock Enterprise Service bezogen.

> Achtung: Um Fernkontrollaktionen auf DriveLock Agenten durchführen zu können, müssen zwingend Berechtigungen definiert werden. Diese werden in den Agentenfernkontroll-Einstellungen und -Berechtigungen definiert.

Die Agenten Fernkontrolle ist nicht verfügbar, wenn Sie den Gruppenrichtlinien-Editor verwenden, um eine DriveLock Gruppenrichtlinie zu editieren. Mit einer lokal installierten DriveLock Management Konsole können Sie die Agenten Fernkontrolle benutzen und Verbindung mit DriveLock Agenten, die z.B. über Gruppenrichtlinie konfiguriert sind, aufnehmen.

4.5.1.1 Agenten-Fernkontroll-Eigenschaften

Um sich die Eigenschaften der Agenten-Fernkontrolle anzeigen zu lassen, rechtsklicken Sie auf den Knoten **Agenten-Fernkontrolle** und wählen anschließend **Eigenschaften**.

Die Option **Agentenliste von DriveLock Enterprise Service beziehen** ist standardmäßig gesetzt.

Bei der Option **Agentenliste automatisch per DNS-SD ermitteln** wird die Liste dynamisch ermittelt und enthält nur Clients die auch online sind.

Sie können die Option **Computer als offline anzeigen, wenn der letzte Kontakt mehr als ... Minuten zurück liegt** nutzen, um das Zeitintervall zu definieren, nachdem ein DriveLock Agent als offline markiert wird. Standard ist hier 15 Minuten.

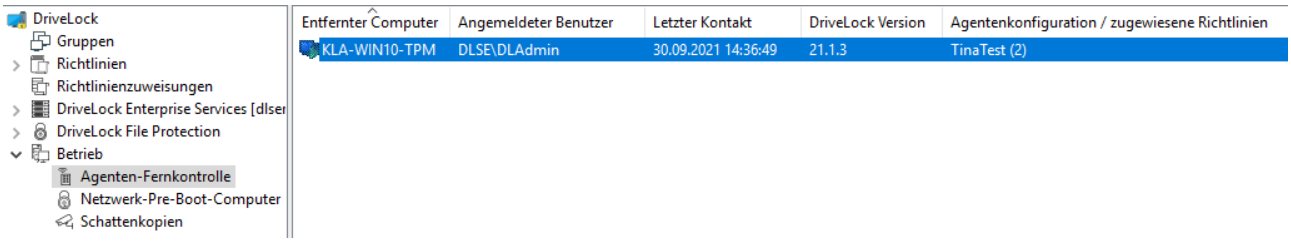
Die Optionen für **Fernsteuerung via DriveLock Enterprise Service (Proxy) verwenden...** regeln das Verhalten der DriveLock Management Konsole beim Verbinden mit einem DriveLock Agenten über die Agenten-Fernkontrolle:

- **Immer** : Die DriveLock Management Konsole stellt die Verbindung ausschließlich über den DriveLock Enterprise Service her.
- **Nie**: Die DriveLock Management Konsole stellt die Verbindung ausschließlich direkt ohne Umweg über den DriveLock Enterprise Service her.
- **Nach Bedarf**: Die DriveLock Management Konsole versucht zunächst, den DriveLock Agenten direkt zu erreichen. Schlägt dieser Versuch fehlt, wird eine Verbindung über den DriveLock Enterprise Service versucht.

Die Verbindung über einen DriveLock Enterprise Service als Proxy spielt nur dann eine Rolle, wenn sich die DriveLock Agenten nicht im gleichen Unternehmensnetzwerk befinden und über einen verknüpften DriveLock Enterprise Service an den zentralen DriveLock Enterprise Service angebunden sind (wie z.B. im Fall eines Security Service Providers – SecaaS).

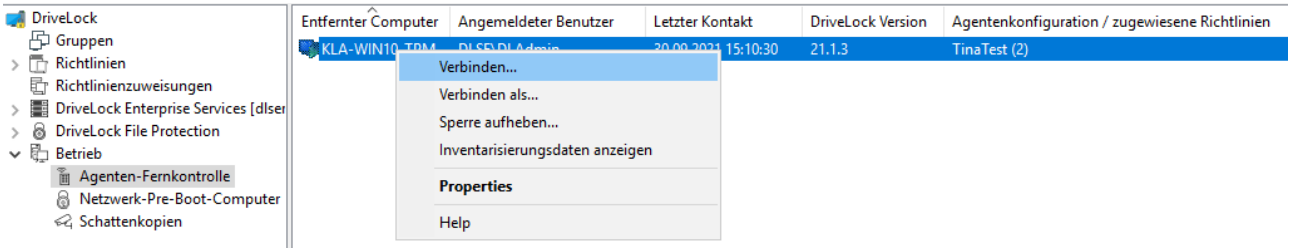
4.5.1.2 Aktive DriveLock Agenten anzeigen

Standardmäßig zeigt die DriveLock Management Konsole im Knoten **Betrieb** unter **Agenten-Fernkontrolle** alle Client-Computer an, die es in der Umgebung finden konnte. Dies funktioniert mithilfe von DNS-SD.



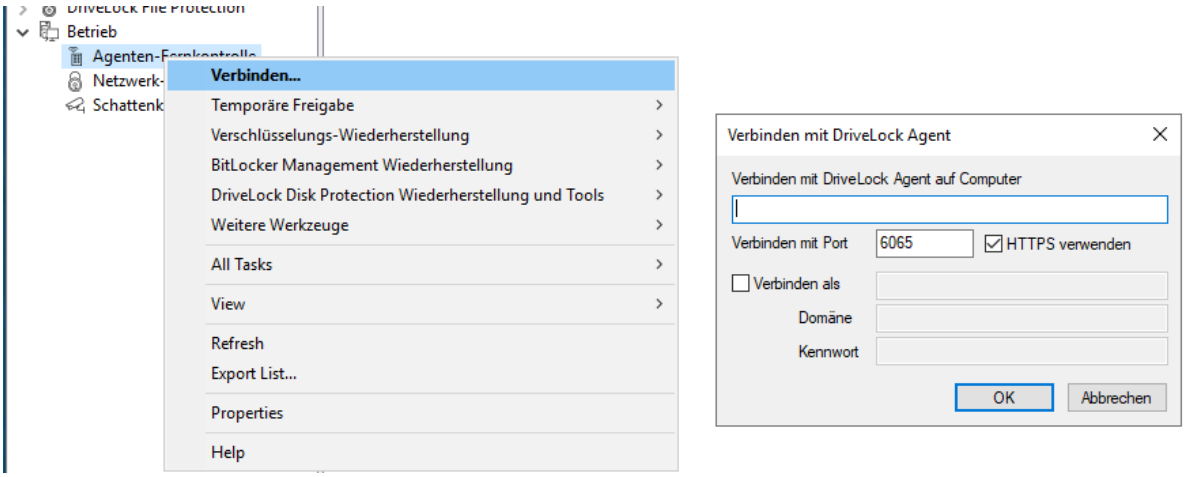
4.5.1.3 Mit einem DriveLock Agenten verbinden

Um Aufgaben an Agenten ausführen zu können, muss zunächst eine Verbindung zum jeweiligen DriveLock Agenten hergestellt werden. Am einfachsten geht das, indem Sie den Agenten auswählen, dann rechtklicken und **Verbinden** aus dem Kontextmenü wählen:



Mit dieser Option wird automatisch der Port 6065 und HTTPS verwendet.

Alternativ dazu kann man über einen Rechtsklick auf den Knoten **Agenten-Fernkontrolle** den Menüpunkt **Verbinden** auswählen und anschließend den Computernamen oder die IP-Adresse eingeben.



> Hinweis: Um eine Verbindung zu einem entfernten Computer aufzubauen, müssen Sie eingehende Verbindungen von TCP Port 6064 und 6065 (Standard) und das Programm DriveLock in den Firewall Einstellungen erlauben.

Nachdem eine Verbindung hergestellt wurde, können Sie die aktuelle Konfiguration auslesen und den DriveLock Agenten kontrollieren.

Kontextmenüeintrag: Verbinden als...

Um einen anderen Port für die Kommunikation zwischen DriveLock Agenten und DES verwenden zu können, wählen Sie den im Kontextmenü des Drivelock Agenten den Menübefehl **Verbinden als...** aus.

Damit die Verbindung mit dem Agenten verschlüsselt wird, ist die Option **HTTPS verwenden** standardmäßig gesetzt. Falls nötig, geben Sie im Dialog korrekte Benutzerdaten ein.

4.5.1.4 Eigenschaften des DriveLock Agenten anzeigen

Durch einen Doppelklick auf den Client-Computer können Sie sich alle Eigenschaften des DriveLock Agenten anzeigen lassen, z.B. die verbundenen Laufwerke und Geräte, temporäre Freigaben, den Verschlüsselungsstatus oder den Status der Applikationskontrolle.

> Hinweis: Im Eigenschaftendialog werden unterschiedliche Reiter angezeigt, je nachdem, welche Lizenzen für den Agenten gelten. Beispielsweise ist der Reiter **Applikationskontrolle** nur dann sichtbar, wenn Sie dieses DriveLock Modul auch lizenziert haben.

Auf dem Reiter **Laufwerke** können Sie alle momentan angeschlossenen Laufwerke des Computers und den momentanen Sperrzustand sehen. Wählen Sie ein Laufwerk aus und klicken auf die Schaltfläche **Details**, um weitere Information anzuzeigen, wie z.B. welche Whitelist-Regeln in Betracht gezogen wurden, oder welche Dateifilter gerade auf dem Laufwerk aktiv sind.

Auf dem Reiter **Allgemein** können Sie eine Aktualisierung der Agenten-Konfiguration durchführen, in dem Sie die Schaltfläche **Richtlinie aktualisieren** klicken. Wenn Sie die Schaltfläche **Temporär freigeben** klicken, öffnet sich der Freigabe-Assistent. Weitere Informationen zur Freigabe finden Sie hier.

Auf dem Reiter **Verschlüsselung** finden Sie eine detaillierte Auflistung der von Ihnen eingesetzten (lizenzierten) Verschlüsselungsmodule und deren Eigenschaften. Außerdem sehen Sie eine Auflistung der verschlüsselten Laufwerke mit dem jeweiligen Verschlüsselungsstatus.

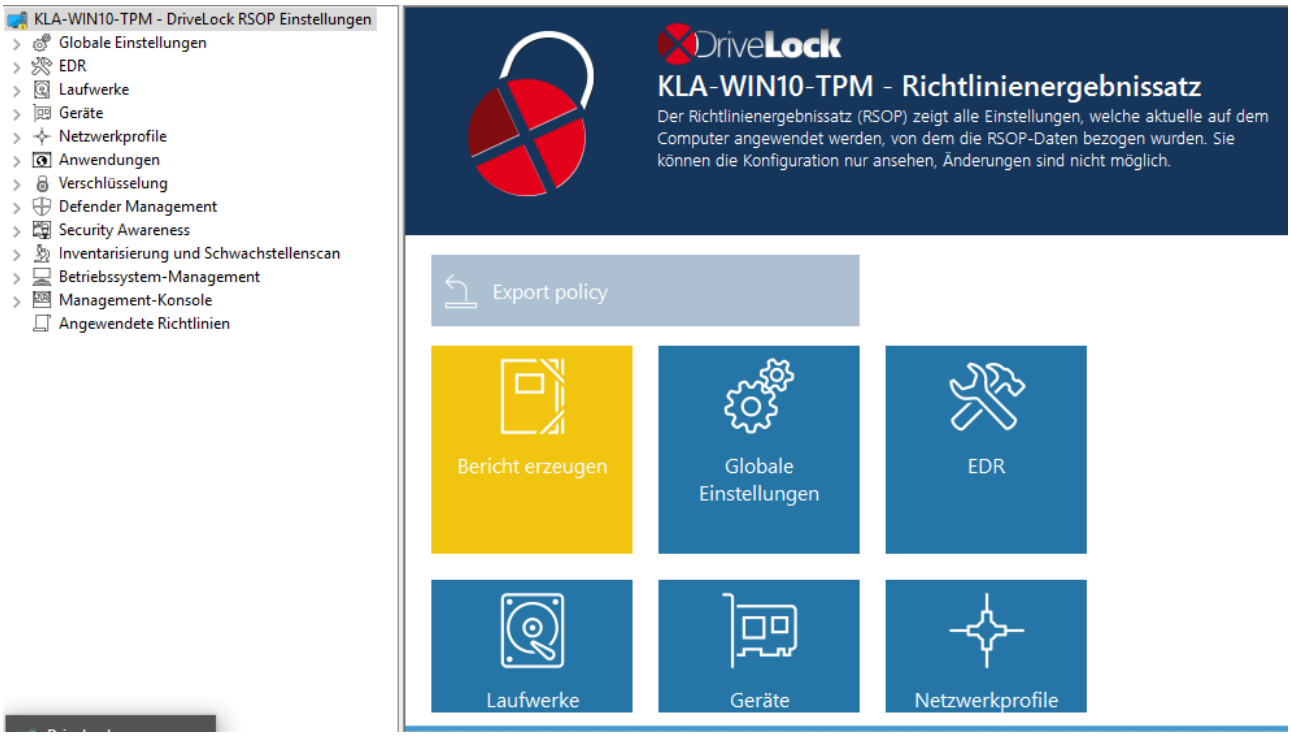
Weitere Informationen zu den jeweiligen Reitern finden Sie in den entsprechenden Kapiteln in diesem Handbuch oder den jeweiligen Dokumentationen auf DriveLock Online Help.

4.5.1.5 Client-Konfiguration auslesen (RSoP)

Um die aktuelle Konfiguration (RSOP = Resultant Set of Policy) eines entfernten Agenten anzuzeigen, rechtsklicken Sie auf den entfernten Computer und wählen **RSOP anzeigen...** aus dem Kontextmenü aus.

Anschließend wird eine extra Konsolen-Fenster geöffnet, das vom Aufbau so aussieht wie der DriveLock Richtlinien-Editor. Um zu überprüfen welche Einstellungen an dem Agenten wirken, erweitern Sie den entsprechenden Knoten und wählen die Einstellung aus.

> Hinweis: Die Einstellungen können nur gelesen aber nicht geändert werden.



Klicken Sie auf **Bericht erzeugen**, um einen Report zu erzeugen, der alle Einstellungen ähnlich einem Report der GPMC anzeigt. Mit STRG + F kann man in der HTML-Ansicht suchen.

4.5.1.6 Inventarisierungsdaten anzeigen

Um die aktuellen Inventarisierungsdaten eines Computers anzuzeigen, rechtsklicken Sie auf den Computer und wählen **Inventarisierungsdaten anzeigen** aus dem Kontextmenü aus. Anschließend werden alle Software- und Hardwaredaten des Computers dargestellt.

Die Datenquelle gibt dabei an, ob die Informationen direkt vom Computer ausgelesen wurden (wenn Sie mit diesem direkt über die Agentenfernkontrolle verbunden sind), oder ob die Daten aus der DriveLock Datenbank über den DriveLock Enterprise Service ausgelesen wurden.

Klicken Sie auf den gewünschten Reiter, um sich die dazugehörenden Informationen anzeigen zu lassen, wie z.B. Informationen zu den installieren Anwendungen oder zu den eingespielten Windows Updates.

4.5.1.7 Verschlüsselungs-Eigenschaften anzeigen

Ähnlich wie auf dem Reiter Verschlüsselung im Eigenschaftendialog des Agenten wird hier der Status der verwendeten Verschlüsselungsoption angezeigt.

Auf dem Reiter **Allgemein** haben Sie folgende Optionen:

Klicken Sie auf die Schaltfläche **Details**, wenn Sie sich Informationen zum verwendeten TPM (sofern verfügbar) anzeigen lassen wollen.

Klicken Sie auf **Agent umkonfigurieren**, wenn Sie Änderungen an der Verschlüsselung des Agenten bzw. an den Pre-Boot-Authentifizierungsseinstellungen vornehmen möchten. Sie können in dem folgenden Dialog abweichend von der zentralen Richtlinie rechnerspezifische Einstellungen konfigurieren. Die gewählten Einstellungen gelten jedoch nur für den gerade verbundenen Computer. Weitere Informationen finden Sie in der DriveLock Encryption Dokumentation auf DriveLock Online Help.

Klicken Sie auf **Wiederherstellungsschlüssel erneut hochladen**, wenn für den Agenten keine Wiederherstellungsdaten am DriveLock Enterprise Service vorhanden sind. Diese Option lädt die lokalen Daten manuell auf den Server hoch.

Auf dem Reiter **Benutzer** sehen Sie, welche Benutzer sich über die Pre-Boot-Authentifizierung am Client-Computer anmelden können (sofern die PBA dort verfügbar ist). Über die Schaltfläche **Hinzufügen** können Benutzer hinzugefügt werden.

4.5.1.8 Lokale Applikationskontroll-Whitelist anzeigen

Sofern Sie eine Lizenz für Application Control erworben haben, können Sie sich mit diesem Befehl den Inhalt der Applikations-Datenbank mit den für diesen DriveLock Agenten freigegebenen Anwendungen mit den entsprechenden Hashwerten anzeigen lassen. Ebenso sehen Sie die verwendeten Zertifikate. Die Informationen können ggf. herauskopiert werden.

4.5.1.9 Debug-Tracing aktivieren

Für die Fehlerbehebung kann eine detaillierte Diagnoseprotokollierung am DriveLock-Agenten aktiviert werden. Diesen Vorgang nennt man Tracing. Mithilfe des Tracing kann der technische Support von DriveLock die Ursache eines Problems feststellen, z.B. wenn Einstellungen nicht so wie erwartet übernommen werden. Sie sollten das Tracing nur für die Fehlerbehebung aktivieren und wieder deaktivieren, sobald Sie die Daten gesammelt haben.

Klicken Sie mit der rechten Maustaste auf den Computer und wählen Sie anschließend **Alle Aufgaben** und dann **Debug tracing**, um das Tracing für den ausgewählten Computer zu aktivieren. Es erscheint eine Hinweismeldung, welche die erfolgreiche Aktivierung bestätigt und den Pfad anzeigt, in dem die Trace-Dateien gespeichert werden.

4.5.1.10 DriveLock Agent temporär freigeben

Mithilfe der temporären Freigabe können Sie schnell und zeitlich begrenzt einem verbundenen DriveLock Agenten den Zugriff auf gesperrte Laufwerke, Geräte oder Anwendungen ermöglichen und/oder die Steuerung von Microsoft Defender deaktivieren.

Dies funktioniert auch für mehrere DriveLock Agenten.

Beispiel: Sie haben standardmäßig alle USB-Laufwerke gesperrt, ein Endbenutzer benötigt aber umgehend Zugriff auf seinen USB-Stick, damit er seine Präsentation zeigen kann. Über die Agenten-Fernkontrolle bekommt der Benutzer innerhalb weniger Minuten Zugriff auf seinen USB-Stick.

Gehen Sie folgendermaßen vor:

1. Entweder klicken Sie die Schaltfläche **Temporär freigeben** im Eigenschaftendialog des Agenten oder den Menübefehl **Temporär freigeben...** aus dem Kontextmenü. Wenn Sie mehrere Agenten freigeben wollen, öffnen Sie den Menübefehl **Mehrere Agenten freigeben...** unter **Temporäre Freigabe** im Kontextmenü des Knotens **Agenten-Fernkontrolle**.
2. Der Freigabe-Assistent wird geöffnet. Wählen Sie im ersten Dialog die freizugebenden Laufwerke bzw. Geräte aus, damit nur das freigegeben wird, was Sie erlauben. Beispiel: Wenn Sie temporär einen USB-Stick freigeben wollen, setzen Sie den Haken bei **Über USB-angeschlossene Laufwerke.**
3. Geben Sie nun die Optionen für die Laufwerkskontrolle an. Erweiterte Zugriffe können temporär durch Setzen der folgenden Optionen für Laufwerke gewährt werden:
   - **Dateifilter während Freigabe abschalten**: Zugriff auf Dateien/Dateitypen zulassen, die sonst durch einen Dateifilter gesperrt wären.
   - **Erzwungene Verschlüsselung deaktivieren**: Zugriff auf Laufwerke zulassen, für die erzwungene Verschlüsselung aktiviert wurde. Weitere Informationen zur erzwungenen Verschlüsselung finden Sie in der DriveLock Encryption Dokumentation auf DriveLock Online Help.
   - **Verwendungsrichtlinie akzeptieren, bevor Zugriff auf Laufwerk erlaubt wird**: Der Benutzer muss einer konfigurierten Verwendungsrichtlinie zustimmen, bevor das Laufwerk freigegeben wird.
   - **Laufwerks-Scan deaktivieren**: Wenn ein Laufwerks-Scan konfiguriert wurde (in den Laufwerks-Whitelist-Regeln), können SIe diesen hier deaktivieren.

4. Sofern Sie die Applikationskontrolle nutzen, können im nächsten Dialog Einstellungen vorgenommen werden, um diese während der Freigabe ebenfalls zu deaktivieren. Zusätzlich legen Sie darüber fest, ob und welche Anwendungsdateien während dieses Freigabezeitraums der lokalen Hash-Datenbank hinzugefügt werden.
   Die Option **Benutzerbestätigung nach Freigabeende für alle Dateien einholen** ermöglicht nach Ende der Freigabe eine manuelle Prüfung aller zuvor neu "gelernten" Anwendungen, bevor diese endgültig in die lokale Anwendungsdatenbank aufgenommen und damit freigegeben werden.
5. Wenn Sie die **Steuerung von Microsoft Defender deaktivieren** wollen, können Sie dies im vorletzten Dialog angeben. Weitere Informationen zu Microsoft Defender Management finden Sie in der entsprechenden Dokumentation auf DriveLock Online Help.

   Hinweis: Beachten Sie bitte, dass hiermit nicht Microsoft Defender deaktiviert wird, sondern lediglich die Verwaltung der Defender-Einstellungen durch DriveLock.

6. Zuletzt wählen Sie den gewünschten Freigabezeitraum aus, entweder in Minuten oder bis zum einem gewünschten Datum und einer Uhrzeit.
   Zusätzlich können Sie als Administrator einen Text (z.B. den Grund der Freigabe) an dieser Stelle eingeben. Dieser Text wird ebenfalls im Ereignis gespeichert und kann über das Reporting ausgewertet werden.
7. Die Freigabe startet sofort nachdem Sie Fertigstellen geklickt haben. Wenn Sie eine Benutzerbenachrichtigung konfiguriert haben, wird diese am Agenten angezeigt.

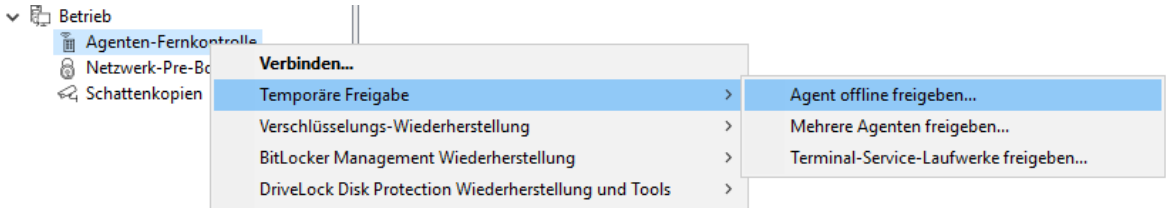
Die Freigabe kann auch vorzeitig beendet werden, indem Sie auf **Freigabe beenden** klicken. Auch hier wird ggf. eine Bestätigung angezeigt.

Offline-Agenten temporär freischalten

Um Agenten freizuschalten, die nicht mit Ihrem Netzwerk verbunden sind, müssen Sie den nachfolgend genannten Schritten folgen. An diesem Prozess sind der Endbenutzer und der Administrator beteiligt, beide haben verschiedene Aufgaben durchzuführen.

Gehen Sie folgendermaßen vor:

1. Rechtsklicken Sie auf **Agenten-Fernkontrolle**, dann **Temporäre Freigabe** und dann **Agent offline freigeben** aus dem Kontextmenü.



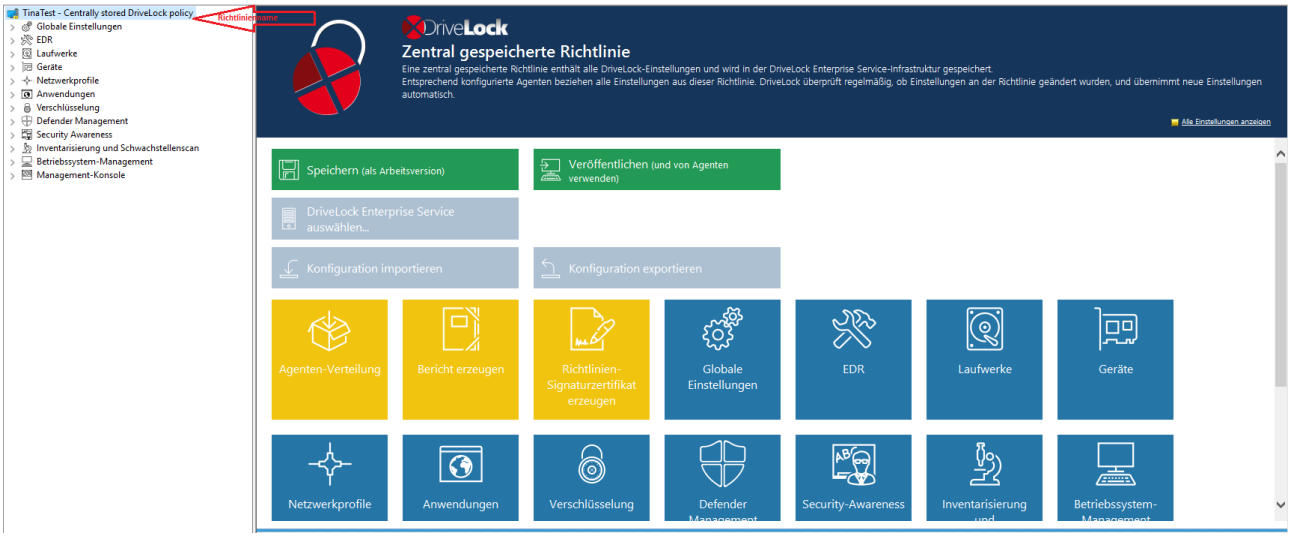
2. Je nachdem, welche Angabe Sie in Ihrer Richtlinie in der Einstellung für die Offline-Freigabe gesetzt haben, geben Sie nun das Kennwort für die Offline-Freigabe ein, oder wählen Sie ein Zertifikat aus. Sie können ein Zertifikat aus einer Datei oder von dem Windows Zertifikatsspeicher des lokalen Computers importieren. Um ein Zertifikat aus einer Datei zu importieren, klicken Sie auf Von Datei importieren und wählen die Zertifikats-Datei aus. Um ein Zertifikat aus dem lokalen Zertifikatsspeicher zu importieren, klicken Sie auf Aus Speicher importieren.
3. Geben Sie den Computernamen und den Anforderungscode ein, den der Benutzer zur Verfügung gestellt hat. DriveLock überprüft die Daten. Wenn der Anforderungscode vor über einer Stunde erstellt wurde, wird das im Feld “Alter des Codes“ dargestellt.
4. Der Code, der vom Benutzer für die Freigabe des DriveLock Agenten zur Verfügung gestellt wird, ist nur für eine Stunde gültig. Wenn diese Zeit überzogen wird, muss der “Computer vorübergehend freigeben” Assistent erneut gestartet werden.
5. Wählen Sie die Zugriffsrechte und den Zeitraum, für den die Freigabe gültig ist.
6. Der Freigabecode wird angezeigt. Der zurückgegebene Freigabecode muss vom Benutzer in die dafür vorgesehenen Felder eingetragen werden.

4.5.1.11 Aktualisierung der Konfiguration

Sie können die Aktualisierung von Gruppenrichtlinien oder das erneute Laden einer Konfigurationsdatei mit Hilfe der DriveLock Management Konsole und der Agentenfernkontrolle manuell erzwingen. Dazu müssen Sie sich wiederum mit dem Agenten verbinden.

5 DriveLock Richtlinien-Editor

Der DriveLock Richtlinien-Editor ist eine Management Konsole, in der Sie alle Einstellungen für Ihre DriveLock Richtlinie konfigurieren können.



Folgende Themen finden Sie unter den jeweiligen Links:

- Globale Einstellungen
- Ereignisse und Alerts
- Betriebssystem-Management
- Management Konsole

Folgende Themen sind aufgrund von derzeitigen Umstrukturierungen der Dokumentation noch im alten **Administrationshandbuch** zu finden:

- Laufwerke
- Geräte
- Netzwerkprofile
- Verschlüsselung mit File Protection

Folgende Themen haben eigenständige Dokumentationen:

- Application Control (Anwendungskontrolle)
- DriveLock Encryption (BitLocker Management, DriveLock PBA, Disk Protection, BitLocker To Go und Encryption 2-Go)
- Defender Management
- DOC Companion

- Inventarisierung und Schwachstellenscan
- Security Awareness

Hinweis: Sie finden diese Themen auf DriveLock Online Help.

5.1 Allgemeine Hinweise

5.1.1 Basis-Einstellungen anzeigen

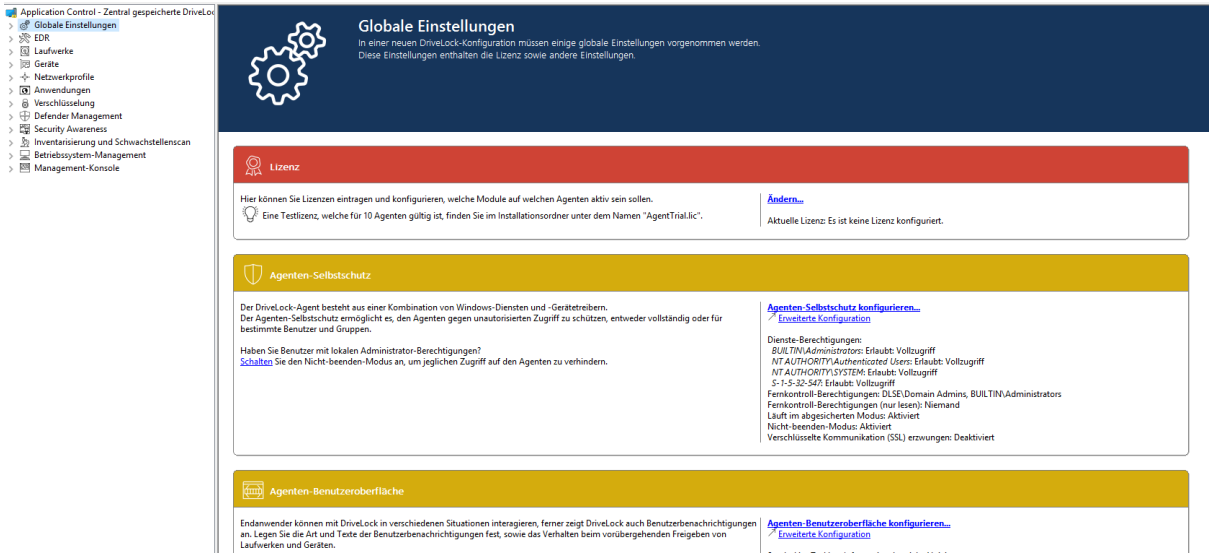
Im obersten Knoten einer Richtlinie können Sie auswählen, mit welchen Einstellungen Sie arbeiten wollen und welche Taskpads Ihnen auf der rechten Seite des Editors angezeigt werden. Die Auswahl betrifft alle Knoten in einer Richtlinie und kann jederzeit geändert werden.

Es gibt zwei Optionen auf oberster Ebene: **Basis-Einstellungen anzeigen** oder **Alle Einstellungen anzeigen**. Je nachdem, welche Auswahl Sie treffen, sehen Sie unterschiedliche Ansichten der Knoten (siehe Beispiel unten für den Knoten **Globale Einstellungen**)

Mit den Basis-Einstellungen können Sie eine schnelle Konfiguration der wichtigsten Parameter erreichen. Wenn diese Ansicht aktiv ist, sind die Taskpads der obersten Knoten in verschiedene Abschnitte unterteilt, die über ihre Farbe anzeigen, ob noch wichtige Einstellungen zu konfigurieren sind (rot), ob die grundsätzlichen Einstellungen konfiguriert wurden aber noch weitere sinnvolle konfiguriert werden sollten (gelb), oder ob bereits alle Einstellungen für einen sicheren Betrieb getroffen wurden (grün).

Tipp: Aus dieser Ansicht heraus können Sie über den Link ↗ Erweiterte Konfiguration. schnell zu allen verfügbaren Einstellungen gelangen.

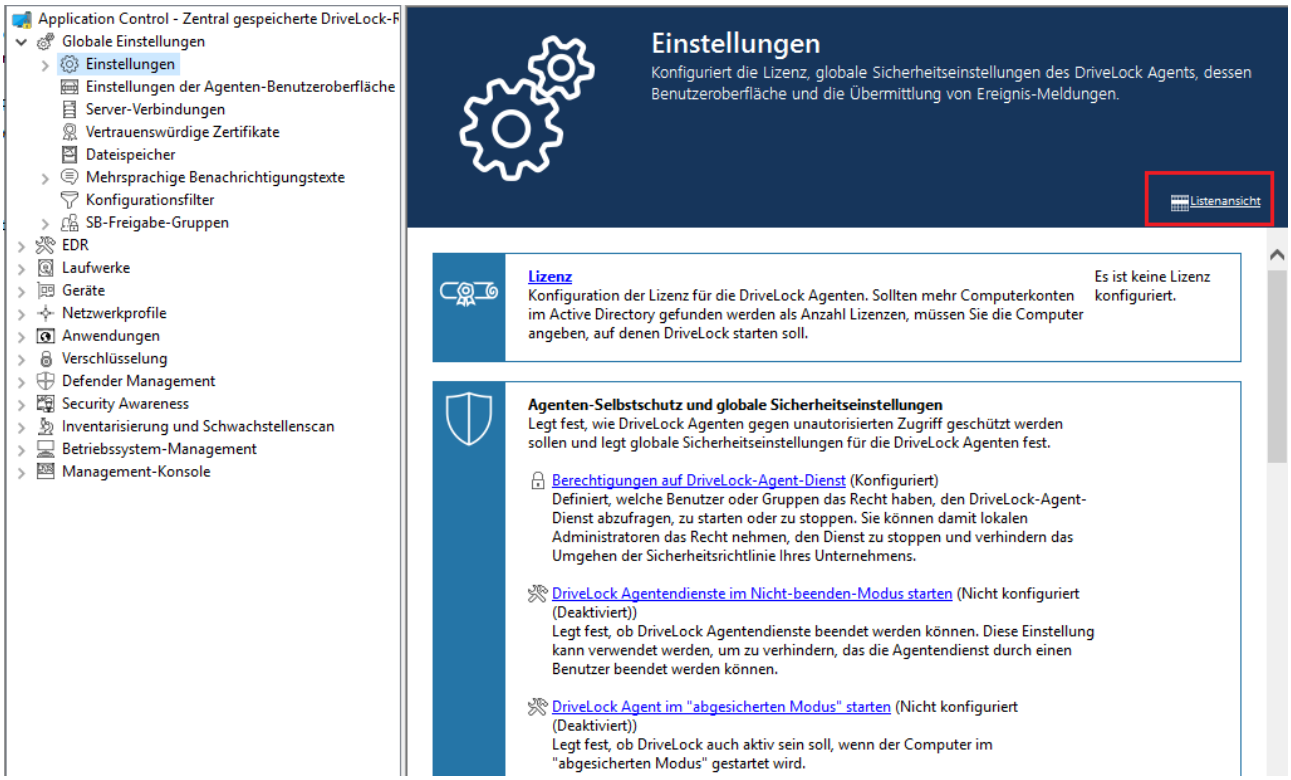
- Ansicht mit aktivierten Basis-Einstellungen:



- Ansicht mit allen Einstellungen:

Bei manchen Knoten in der Management Konsole bzw. im Richtlinien-Editor haben Sie außerdem noch die Möglichkeit, von einer benutzerfreundlichen und strukturierten **Task-pad-Ansicht** zu einer einfachen **Listenansicht** zu wechseln.

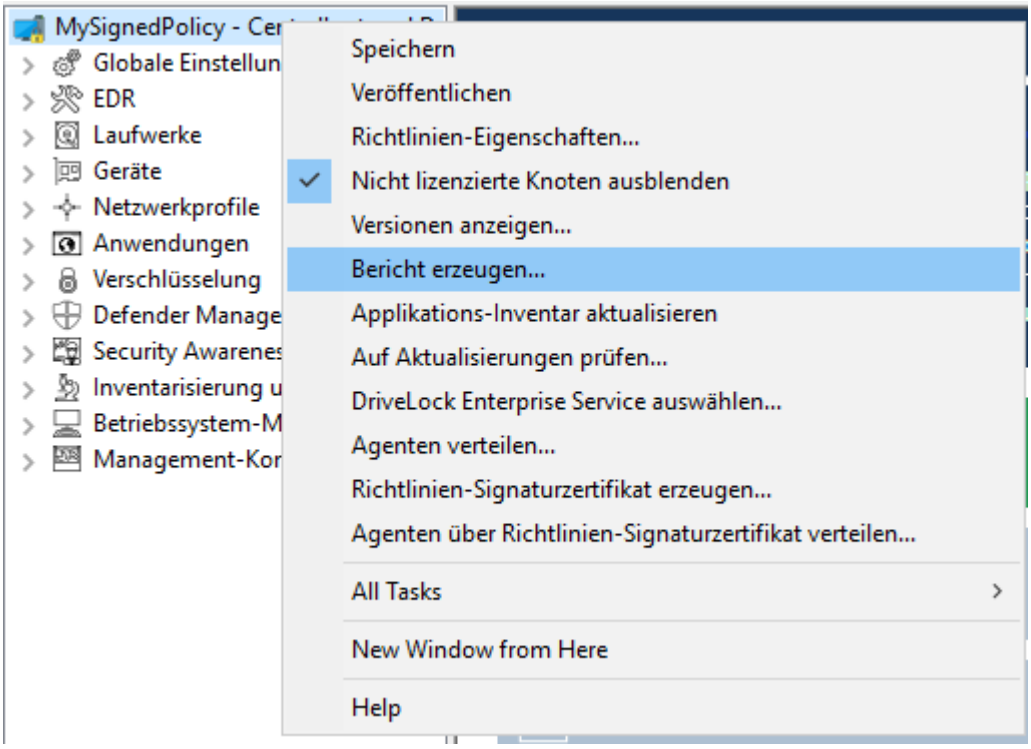
Hier die Taskpad-Ansicht am Beispiel des Knotens **Einstellungen**:



5.1.2 Konfigurationsbericht erzeugen

DriveLock kann einen XML-basierten Bericht erzeugen, der alle Konfigurationseinstellungen ähnlich einem Gruppenrichtlinienbericht enthält. Sie können diesen Bericht anzeigen, speichern oder ausdrucken.

Klicken Sie auf **Bericht erzeugen...**, um einen Konfigurationsbericht zu generieren.



Verwenden Sie den Scrollbalken und die „+“ und „-“ Symbole, um durch den Bericht zu navigieren.

Klicken Sie Bericht speichern, um ihn als „*.html“ Datei zu speichern. Sie können z.B. den Internet Explorer zur Ansicht verwenden.

Klicken Sie auf Drucken, um den Bericht auszudrucken. Es öffnet sich ein neues Internet Explorer Fenster und das Druckmenü öffnet sich. Wählen Sie einen Drucker und klicken Sie Drucken.

5.1.3 Richtlinien-Signaturzertifikat

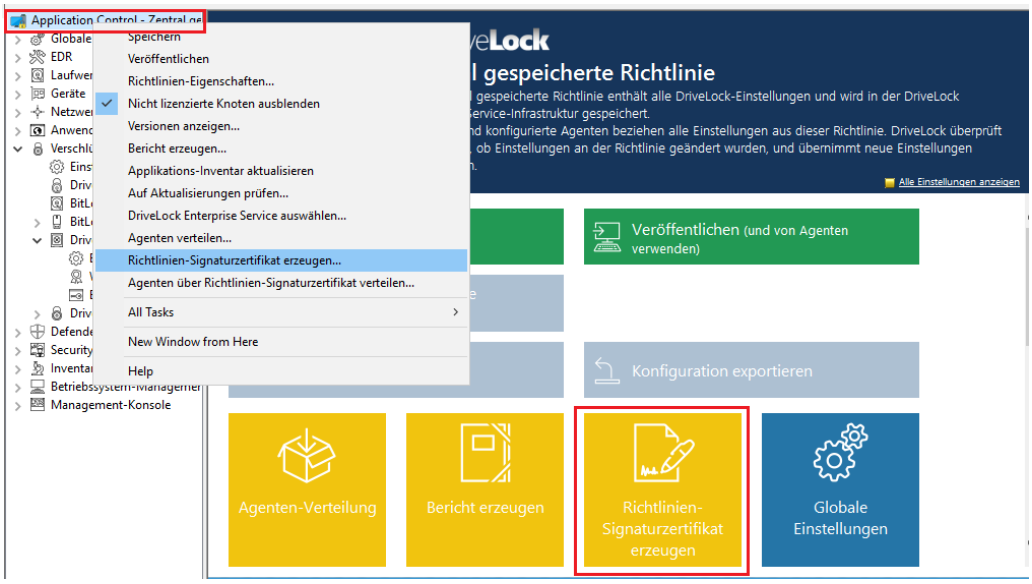
Sie können zentral gespeicherte Richtlinien mit einem Zertifikat signieren, um die Verteilung von Richtlinien auf DriveLock Agenten zusätzlich abzusichern. Durch die Verwendung von Signaturzertifikaten können Sie sicherstellen, dass ein DriveLock Agent nur die ihm zugewiesenen signierten Richtlinien erhält und diese auf dem Weg vom DriveLock Enterprise Service (DES) zum Agent nicht verändert werden. Einige Sicherheitszertifizierungen setzen Signaturzertifikate voraus.

Beachten Sie bitte folgendes:

- Ein DriveLock Agent, der noch nicht konfiguriert wurde, kann unsignierte und signierte Richtlinien verwenden
- Sobald ein Agent so konfiguriert ist, dass dieser nur signierte Richtlinien verwendet, werden unsignierte Richtlinien ignoriert
- Im Signaturzertifikat wird die komplette Agentenkonfiguration gespeichert
    - DES-Server
    - Mandant
    - Richtlinientyp
    - Zusätzliche Zertifikate
    - Notfall-Richtlinie
- Diese Konfiguration kann nur mit einem neuen, anderen Signaturzertifikat geändert werden
- Ein für die Verwendung von signierten Richtlinien konfigurierter Agent ignoriert die manuelle Neukonfiguration über DOC

5.1.3.1 Signaturzertifikat erzeugen

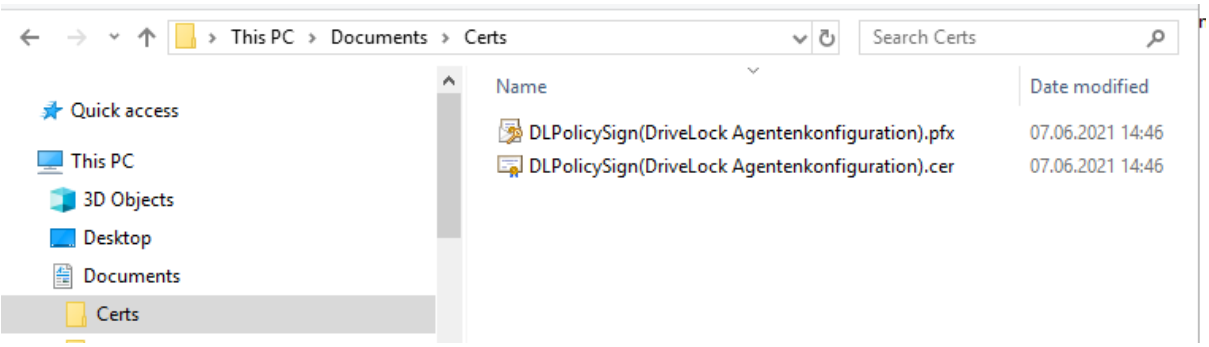
Ein Zertifikat wird innerhalb des DriveLock Richtlinien-Editors erzeugt. Wählen Sie dazu aus dem obersten Navigationsknoten den Menübefehl **Richtlinien-Signaturzertifikat erzeugen...**.



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

1. Wählen Sie den Speicherort für das generierte Zertifikat aus. Sie können optional das Zertifikat auch auf einer Smartcard abspeichern.
2. Für den Zugriff auf das Zertifikat bzw. den privaten Schlüssel benötigen Sie später ein Kennwort. Legen Sie dieses fest.
3. Im nächsten Schritt können Sie eine oder mehrere Serververbindungen und einen Mandanten konfigurieren, sofern Sie mit mehreren Mandanten arbeiten. Ebenso können Sie festlegen, dass ein DriveLock Agent, der mit diesem Zertifikat installiert wird, immer eine ganz bestimmte Richtlinie verwendet, unabhängig davon welche Zuweisung Sie in der DriveLock Management Console für die Richtlinien vorgenommen haben.
4. Im letzten Schritt legen Sie fest, ob der mit diesem Zertifikat installierte Agent noch weitere Richtlinien akzeptiert, die mit den hier anzugebenden anderen Zertifikaten signiert wurden.
5. Außerdem können Sie eine Konfiguration aus einer Konfigurationsdatei hinzufügen, die ein Agent verwendet, solange er keine Richtlinie über einen DES oder eine Gruppenrichtlinie erhält.

6. Beenden Sie den Assistenten. Im angegebenen Speicherort befinden sich folgende Zertifikats-/Schlüssel-Dateien:



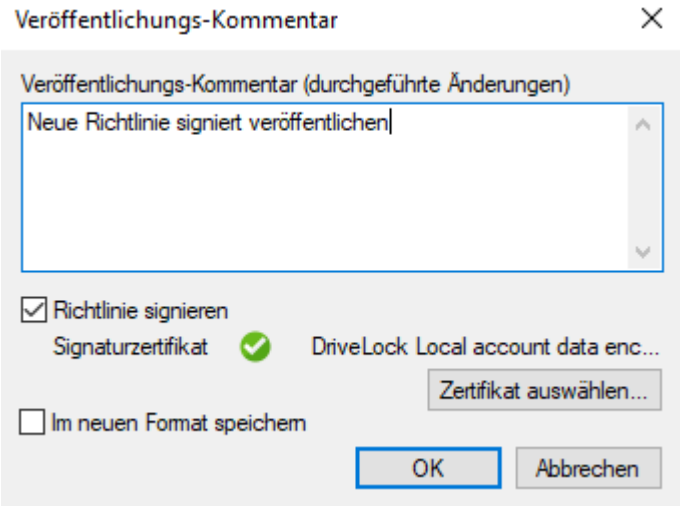
5.1.3.2 Richtlinie signieren

Gehen Sie folgendermaßen vor:

1. Zunächst müssen Sie die Richtlinie, die Sie signieren wollen, veröffentlichen.
2. Im Veröffentlichungsdialog geben Sie einen entsprechenden Kommentar ein, aktivieren Sie **Richtlinie signieren** und klicken Sie **Zertifikat auswählen...**.

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

3. Wählen Sie das zuvor generierte Zertifikat bzw. dessen private Schlüsseldatei aus, geben Sie das passende Kennwort ein und klicken Sie OK.
4. Ein Symbol zeigt Ihnen die erfolgreiche Signatur an. Klicken Sie auf OK, um die signierte Richtlinie zu veröffentlichen.

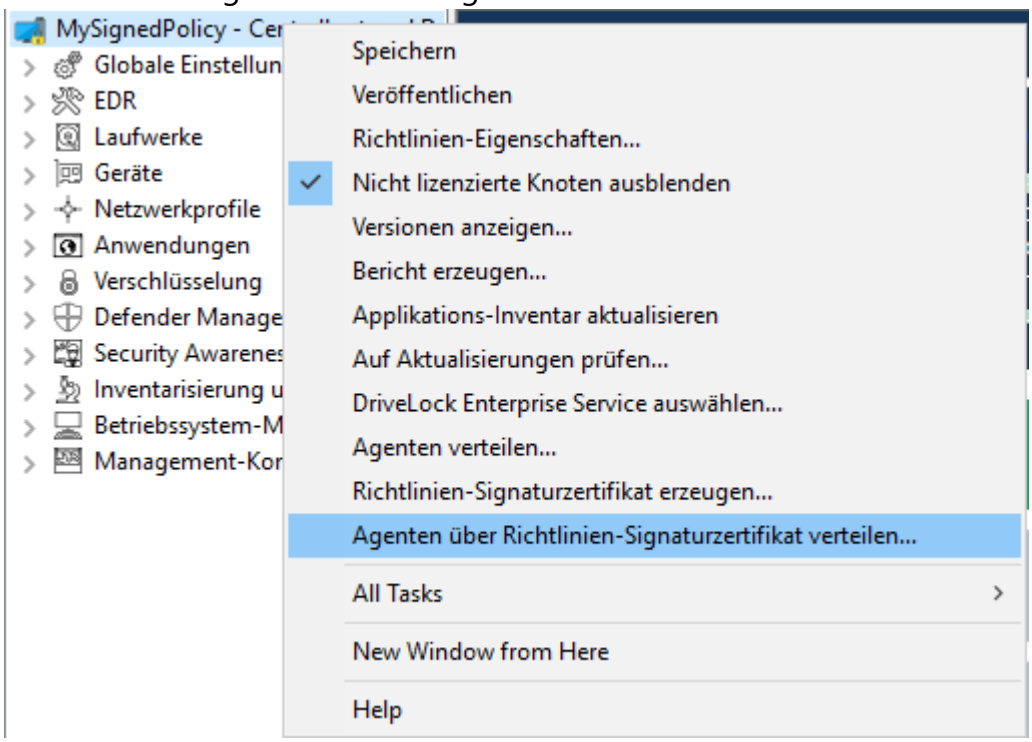


5.1.3.3 Signierte Richtlinie verteilen

Nachdem Sie mindestens ein Zertifikat erzeugt, dieses signiert und dann die signierte Richtlinie veröffentlicht haben, müssen folgende Schritte durchführt werden, um einen DriveLock Agenten mit dem Richtlinien-Signaturzertifkat zu installieren.

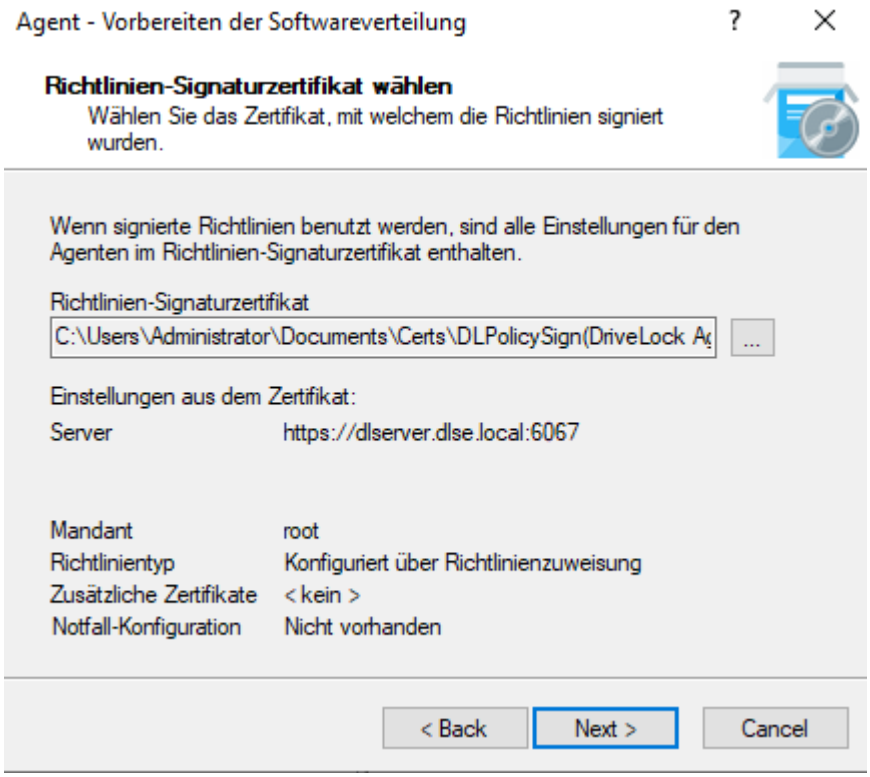
Detaillierte Informationen zur Installation von DriveLock Agenten finden Sie im Installationshandbuch auf DriveLock Online Help.

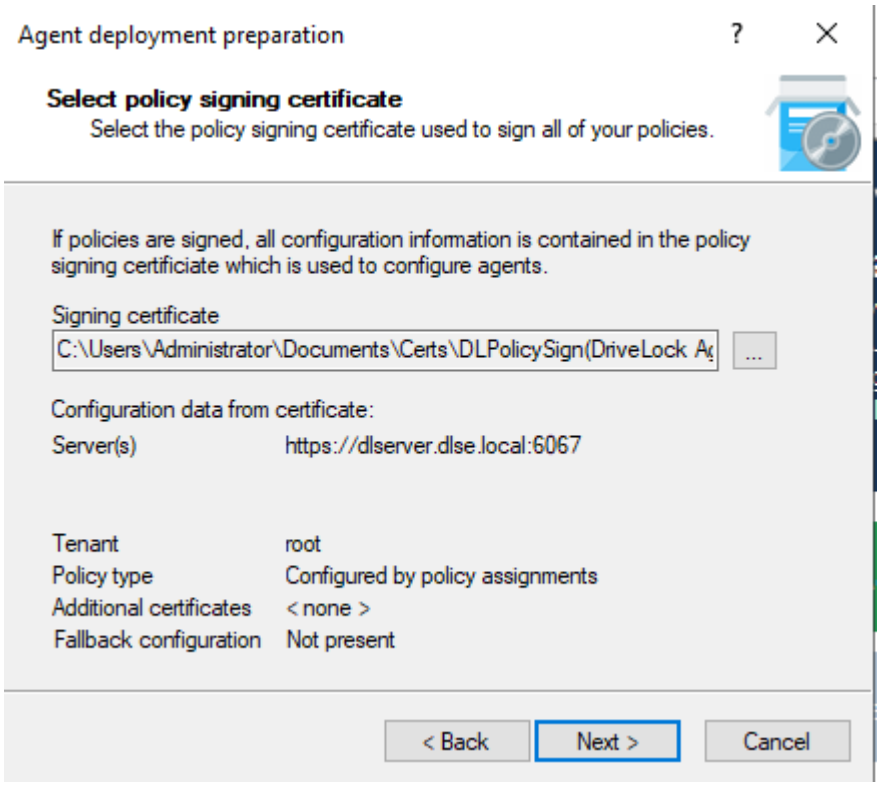
1. Öffnen Sie das Kontextmenü der Richtlinie in der DriveLock Management Console und wählen Sie **Agenten über Richtlinien-Signaturzertifikat verteilen**, um den Assistenten für die Agenten-Verteilung zu starten.



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

3. Wählen Sie im nächsten Dialog das Richtlinien-Signaturzertifikat aus, mit dem die DriveLock Richtlinie signiert wurde. Nach der Auswahl werden Ihnen die im Zertifikat gespeicherten Informationen angezeigt.





4. Wählen Sie die Art des Installationspakets
   - Windows Installer Paket (MSI): Erstellt ein neues Microsoft Installer Paket, das die zuvor spezifizierten Einstellungen enthält

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

5. Geben Sie Quelle und Ziel für das Paket an.
6. Sie können nun das generierte Installationspaket z.B. über die Softwareverteilung Ihres Unternehmens verteilen.

Manuelle Konfiguration des Agenten über die Befehlszeile

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

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

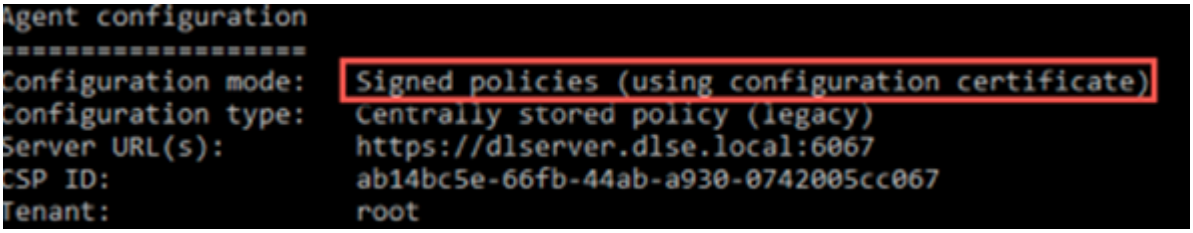
Wenn Sie einen bereits installieren Agenten umkonfigurieren möchten, dass er nur noch mit einem bestimmten Zertifikat signierte Richtlinien akzeptiert, können Sie das mit folgenden Kommandozeilenbefehl bewerkstelligen:

```
drivelock -setconfigcert "<PATHTOCERTIFICATE>\<Po-
licySigningCertificate>.cer"
```

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

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

```
drivelock -showstatus
```



5.2 Globale Einstellungen

Im Knoten **Globale Einstellungen** können Sie modulunabhängige Einstellungen definieren.

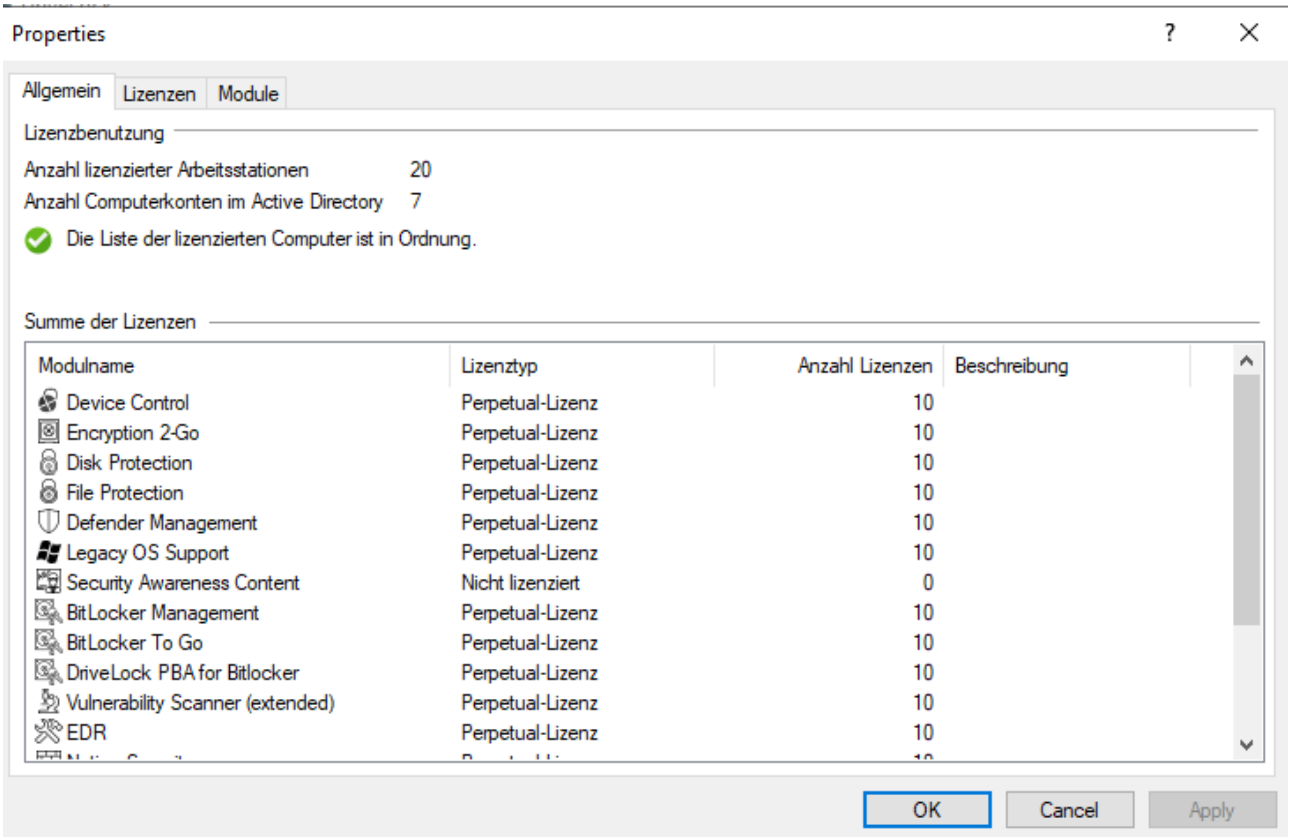
Sie wirken für alle Agenten, die diese Konfiguration benutzen, unabhängig davon ob sie über GPO, zentral gespeicherte Richtlinie oder Konfigurations-Datei angegeben wurden.

5.2.1 Einstellungen

5.2.1.1 Lizenz

Sofern Sie einen DriveLock Enterprise Service (DES) installiert haben, sollten Sie die Lizenzinformationen direkt an diesen übertragen. Bestimmte Server-Funktionen, z.B. das Herunterladen des Security Awareness Content AddOn, können nur dann aktiviert werden, wenn eine gültige Lizenz auf dem DES vorhanden ist.

Klicken Sie auf **Ändern...**, um den Lizenzdialog zu öffnen.



Auf dem Reiter **Allgemein** wird der Lizenzstatus der einzelnen Module angezeigt.

Auf dem Reiter **Lizenzen** können Sie Ihre Lizenzdatei oder den Lizenzschlüssel hinzufügen oder ggf. abgelaufene oder Test-Lizenzen entfernen.

Führen Sie die Schritte zur Lizenzaktivierung im Assistenten durch.

Die DriveLock Lizenz kann entweder online oder manuell durch einen Anruf beim DriveLock Aktivierungscenter aktiviert werden. Für eine Online-Aktivierung wählen Sie **Online**. Wenn die Angabe eines Proxy-Servers für Ihre Internetverbindung notwendig ist, klicken Sie auf **Proxy** und geben den Servernamen, einen Benutzer und das passende Kennwort ein.

Die Lizenz wird aktiviert, indem eine Verbindung mit dem DriveLock Aktivierungsserver aufgenommen wird. Dies dauert in der Regel nur ein paar Sekunden.

Hinweise für die telefonische Aktivierung:

1. Um Unstimmigkeiten zu vermeiden, stellen Sie bitte sicher, dass der Computer, den Sie für die Aktivierung verwenden, eine aktuelle Uhrzeit und die korrekte Zeitzone besitzt.
2. Der Aktivierungscode ist nur für einen bestimmten Zeitraum gültig. Sie müssen den Aktivierungscode innerhalb einer Stunde eingeben, ansonsten müssen Sie einen

neuen Aktivierungscode anfordern. Falls das passieren sollte, klicken Sie auf Abbrechen und starten den Aktivierungs-Assistenten erneut.

Hinweis: Wir empfehlen nach einer erfolgreichen Aktivierung, die Lizenzen an den DriveLock Enterprise Service zu übertragen. Geben Sie an dieser Stelle den Servernamen an, auf dem Ihr DriveLock Enterprise Service installiert ist. Wenn Sie keinen Namen angeben, wird der Übertragungsvorgang übersprungen.

Um den Inhalt einer Lizenz anzusehen, markieren Sie die gewünschte Lizenz und klicken Sie auf **Eigenschaften...**.

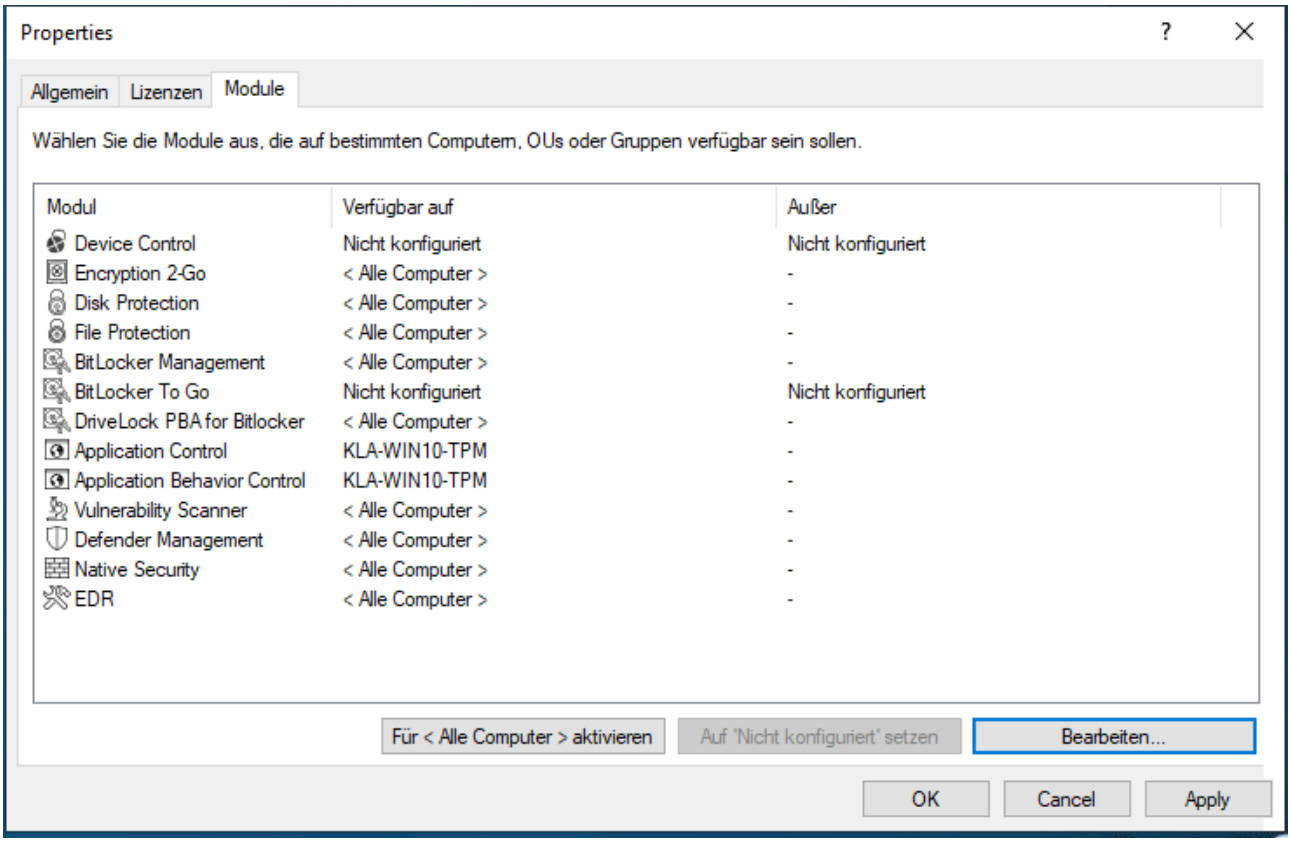
Auf dem Reiter **Module** können Sie konfigurieren welches Modul auf welchen Agenten aktiv sein soll.

Durch diese Angaben können Sie...

- vermeiden, dass ein bestimmtes Modul auf zu vielen DriveLock Agenten verwendet wird (nur aktive Module "verbrauchen" eine Lizenz)
- vermeiden, dass auf einem Agenten Module initialisiert werden, die dort nicht benötigt werden.

Wenn Sie Module auf den Wert nicht konfiguriert setzen, werden die Einstellungen aus einer andere Richtlinie verwendet. Dies bedeutet, dass Sie unterschiedliche Module auch in unterschiedlichen Richtlinien konfigurieren können, als nur in der Richtlinie, in der Sie die Lizenz eintragen.

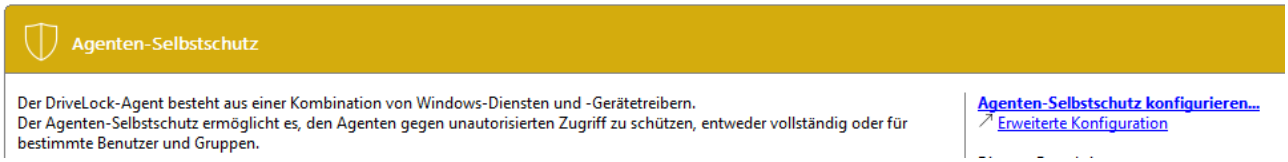
Hinweis: Die Gesamtzahl der benötigten Lizenzen wird anhand der Agentenrückmeldungen ermittelt. Sie werden darauf aufmerksam gemacht, wenn Sie zu wenig Lizenzen haben.



5.2.1.2 Agenten-Selbstschutz und globale Sicherheitseinstellungen

Agenten-Selbstschutzmechanismen schützen davor, dass Benutzer die konfigurierten Sicherheitseinstellungen von DriveLock umgehen können.

Sie können entweder über den Agenten-Selbstschutz-Assistenten schnell grundlegende Konfigurationsschritte vornehmen, indem Sie auf **Agenten-Selbstschutz konfigurieren...** klicken:



Alternativ können Sie über die **Erweiterte Konfiguration** folgende Einstellungen separat setzen:

Berechtigungen auf DriveLock-Agent-Dienst

DriveLock Agentendienste im Nicht-beenden-Modus starten

DriveLock Agent im "abgesicherten" Modus starten

Kennwort zum Deinstallieren von DriveLock

Agentenfernkontroll-Einstellungen und -Berechtigungen

5.2.1.2.1 Berechtigungen auf DriveLock-Agent-Dienst

Mit dieser Option können Sie die DriveLock-Dienst Berechtigungen individuell und gezielt festlegen, beispielsweise um bestimmten Benutzern den Zugriff auf den Dienst zu verweigern oder um den DriveLock (Agenten) Dienst zu kontrollieren (z.B. verweigern Sie der Gruppe „Hauptbenutzer“ die Möglichkeit, den Dienst zu stoppen).

Um einzustellen, welche Benutzer den DriveLock Dienst auf den Client Rechnern stoppen dürfen, können Sie hier die entsprechenden Berechtigungen konfigurieren. Sie sollten zum Beispiel den Hauptbenutzern das Recht entziehen, den DriveLock Dienst anzuhalten.

Sie können die folgenden Aktionen für Benutzer und Gruppen zulassen (oder verweigern):

- Dienst-Informationen lesen: Zeigt die Eigenschaften des Dienstes an.
- Dienst starten / stoppen
- Vollzugriff

> Achtung: Sie können dem Konto “Lokales System” (SYSTEM)” keine Rechte entziehen. DriveLock wird die entsprechenden Rechte automatisch wiederherstellen. Es ist zwingend notwendig, dass das Systemkonto die entsprechenden Rechte auf den DriveLock Dienst hat.

5.2.1.2.2 DriveLock Agentendienste im Nicht-beenden-Modus starten

Wenn Sie keine individuellen Berechtigungen vergeben und stattdessen den DriveLock Agenten-Dienst komplett absichern wollen, benutzen Sie diese Option.

> Achtung: Diese Einstellung führt dazu, dass der Agenten-Dienst durch keinen Benutzer mehr beendet werden kann, unabhängig davon, welche Einstellungen Sie bei der individuellen Berechtigungskonfiguration vorgenommen haben. Bitte beachten Sie, dass eine Deinstallation des Agenten bei aktiviertem Nicht-Beenden-Modus nicht möglich ist.

5.2.1.2.3 DriveLock Agent im "abgesicherten" Modus starten

Klicken Sie auf DriveLock Agent im abgesicherten Modus starten, um festzulegen, ob DriveLock auch im Abgesicherten Modus von Windows ausgeführt werden soll oder nicht.

Achtung: Wenn diese Option aktiviert wird, ist es nicht mehr möglich ist, zu einer vorherigen DriveLock Konfigurationseinstellung im abgesicherten Modus von Windows zurückzukehren.

5.2.1.2.4 Kennwort zum Deinstallieren von DriveLock

Um zu verhindern, dass ein DriveLock Agent ohne Erlaubnis auf einem Computer deinstalliert wird, können Sie hier zum Schutz ein Kennwort für die Deinstallation vergeben.

Wenn die Option **Nicht konfiguriert** gesetzt ist, wird kein Kennwort benötigt, um Agenten zu deinstallieren.

Wenn Sie einen DriveLock Agenten mit Kennwort deinstallieren wollen, müssen Sie den folgenden Befehl ausführen:

```
msiexec /x DriveLockAgent.msi UNINSTPWD= your password
```

Achtung: Das Kennwort für die Installation ist nur für DriveLock Agenten anwendbar. Die komplette Installation von DriveLock kann nicht mit diesem Kennwort geschützt werden.

Achtung: Es wird empfohlen, die Standardeinstellung **Nicht konfiguriert** zu übernehmen, wenn Sie DriveLock Agenten in Ihrem Netzwerk aktualisieren wollen.

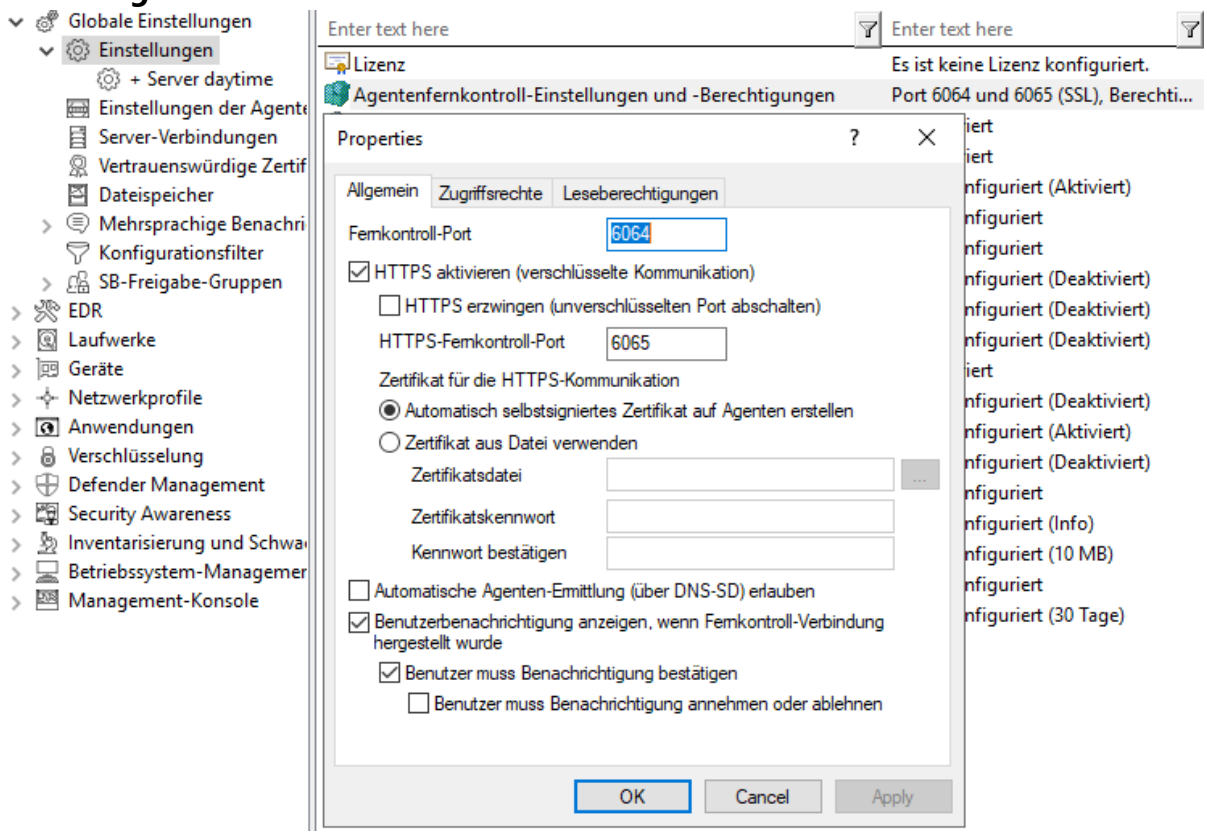
5.2.1.2.5 Agentenfernkontroll-Einstellungen und -Berechtigungen

Achtung: Um Fernkontrollaktionen auf DriveLock Agenten durchführen zu können, müssen zwingend Berechtigungen definiert werden.

Unter **Agentenfernkontroll-Einstellung und -Berechtigungen** lassen sich unterschiedliche Berechtigungen für Benutzer festlegen (siehe Abbildung), um DriveLock Agenten aus der Ferne kontrollieren zu können. Außerdem legen Sie hier weitere Verbindungseinstellungen fest.

- Reiter **Leseberechtigungen**: hier geben Sie Benutzer oder Gruppen an, die bei Fernverbindungsaktionen Informationen von DriveLock Agenten ausschließlich abfragen dürfen.
- Reiter **Zugriffsrechte**: hier geben Sie Benutzer oder Gruppen an, die explizit Aktionen auf dem Agenten ausführen dürfen, beispielsweise einen Agenten temporär freigeben oder Änderungen an der Konfiguration vornehmen können.

- Reiter **Allgemein**:



  - Der Fernkontroll-Port 6064 ist für unverschlüsselte bzw. 6065 für verschlüsselte Verbindungen eingestellt. Sie können diese Ports bei Bedarf ändern. Die Einstellung **HTTPS aktivieren (verschlüsselte Kommunikation)** ist standardmäßig gesetzt.

> Hinweis: Aus Sicherheitsgründen empfehlen wir dringend, diese Einstellung zu verwenden. DriveLock Agenten verweigern somit unverschlüsselte Verbindungen.

  - Normalerweise verwendet DriveLock ein automatisch generiertes und selbstsigniertes Zertifikat für die HTTPS-Verbindung. Wählen Sie die Option **Zertifikat aus Datei verwenden**, um ein anderes Zertifikat zu verwenden, welches Sie anschließend über die Schaltfläche ... auswählen können. Sofern der private Schlüssel des Zertifikats durch ein Kennwort geschützt ist, geben Sie dieses zwei Mal ein.
  - Wenn Sie die Option **Benutzerbenachrichtigung anzeigen, wenn Fernkontroll-Verbindung hergestellt wurde** ausgewählt haben, erhält der aktuell angemeldeten Benutzer auf dem Zielrechner eine Benachrichtigung über den erfolgten Fernkontrollzugriff.

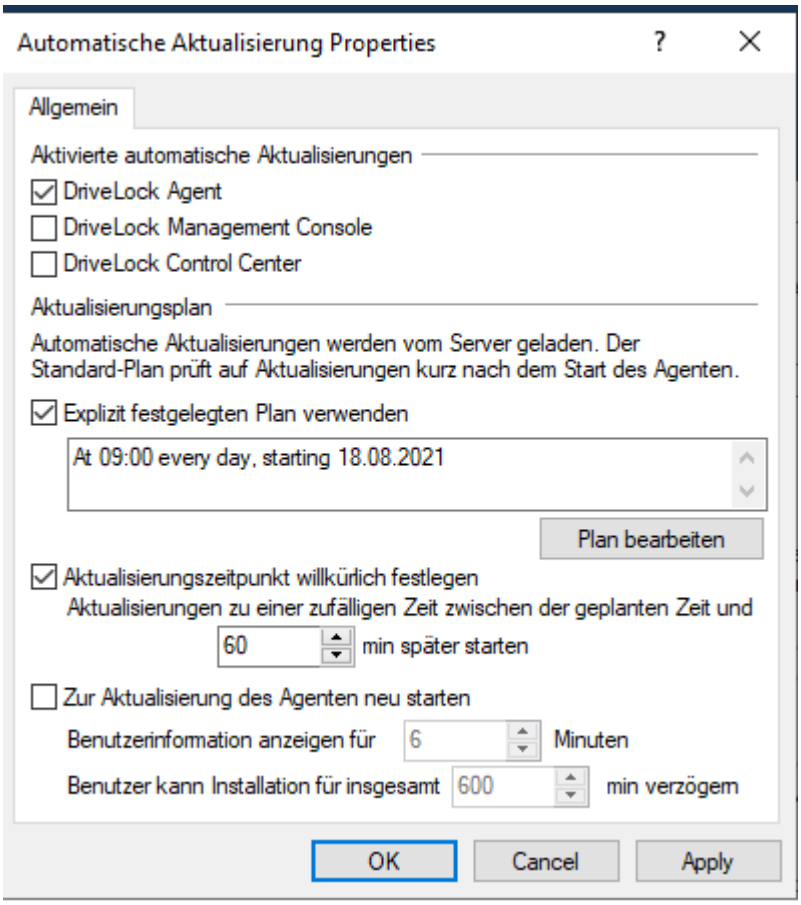
5.2.1.3 Einstellungen zur Übermittlung von Ereignis-Meldungen

Informationen zu diesem Thema finden Sie hier im Kapitel Ereignisübermittlung unter Ereignisse und Alerts.

5.2.1.4 Automatische Aktualisierung

DriveLock Agenten können sich und weitere Komponenten automatisch auf eine neuere Version aktualisieren.

Markieren Sie unter **Aktivierte automatische Aktualisierungen** die Komponenten, die Sie automatisch aktualisieren möchten.



In der Standardeinstellung prüft der Agent dann zufällig innerhalb von 60 Minuten nach dem Systemstart und danach weiterhin alle 60 Minuten, ob neuere Versionen am DES vorhanden sind. Wenn ja, wird der DES diese sofort herunterladen und installieren. Durch die zufällige Zeitspanne ist gewährleistet, dass nicht alle Rechner eines Unternehmens gleichzeitig mit der Aktualisierung bzw. mit dem Download des Installationspaketes beginnen.

Sie können auch eigene Zeitpläne festlegen und eine eigene zufällige Zeitspanne zum eingestellten Aktualisierungszeitpunkt hinzuaddieren.

Während der Aktualisierung ist DriveLock für kurze Zeit inaktiv. Wollen Sie sicherzustellen, dass das System während der Aktualisierung nicht in Benutzung ist, markieren Sie **Zur Aktualisierung des Agenten neu starten**. Der Benutzer kann dann die Aktualisierung um maximal N Minuten verzögern. Wenn er vorher zustimmt oder die Zeit abgelaufen ist, wird er abgemeldet und die Aktualisierung wird vor dem Neustart durchgeführt.

5.2.1.5 DriveLock Simulationsmodus einstellen

Der DriveLock Simulationsmodus ermöglicht es Ihnen, DriveLock zu installieren und die Konfiguration zu verteilen, ohne dass Beeinträchtigungen der Anwender durch das Sperren von Laufwerken, Geräten oder Anwendungen entstehen können.

Typischerweise wird der Simulationsmodus verwendet, indem eine einfache DriveLock Richtlinie mit aktiviertem Simulationsmodus erstellt und verteilt wird. Nachdem diese angewendet wurde, können Sie die entsprechenden DriveLock Ereignisse untersuchen oder sich mit Anwendern besprechen, um Einstellungen zu identifizieren, die angepasst werden sollten. Sobald Sie sicher sind, dass Ihre Richtlinie wie benötigt funktioniert, können Sie den Simulationsmodus deaktivieren.

Wenn der Simulationsmodus aktiv ist, verhält sich DriveLock wie folgt:

- DriveLock sperrt keine externen Laufwerke, Geräte, Anwendungen und Netzwerkverbindungen.
- Der Dateifilter ist deaktiviert.
- Ereignismeldungen werden erzeugt und entsprechend der Konfiguration weitergeleitet.
- Benutzerbenachrichtigungen werden wie konfiguriert erzeugt.
- Erzwungene Verschlüsselung ist aktiviert, unverschlüsselte Laufwerke werden wie konfiguriert verschlüsselt.
- Alle anderen Funktionen verhalten sich normal.

Hinweis: Standardmäßig ist der Simulationsmodus deaktiviert.

5.2.1.6 Erweiterte Einstellungen

Dies sind spezielle Einstellungen für die Kommunikation mit dem DriveLock Agenten.

5.2.1.6.1 Fernzugriff in der Windows Firewall erlauben

Diese Option ist standardmäßig aktiviert.

Die TCP Ports 6064 (HTTP) und 6065 (HTTPS - Standardport) müssen in der Firewall freigegeben sein, damit die Agentenfernkontrolle möglich ist.

> Achtung: Falls Sie diese Einstellung später auf Deaktiviert setzen, bleiben die Ports dennoch aktiviert.

5.2.1.6.2 Konfigurationseinstellungen für Textnachrichten (SMS)

Diese Einstellung konfiguriert das SMS-Gateway, das DriveLock Agenten zum Senden von Textnachrichten verwenden sollen. Sie wird gesetzt, wenn Sie Encryption 2-Go verwenden und das Verschicken von Kennwörtern für neu erstellte, verschlüsselte Container einsetzen wollen.

> Hinweis: Sie müssen Ihr Gateway, Ihren Provider, die Authentifizierungsangaben und die passenden API Parameter kennen und entsprechend eintragen. Diese Werte sind unabhängig von DriveLock.

Die **Gateway-URL** ist firmenintern konfigurierbar und muss entsprechend angegeben werden.

Geben Sie an, ob Sie **GET** oder **POST** verwenden. Testen Sie ggf. die Verbindung.

5.2.1.6.3 Wenn Benutzer impersoniert werden: "Netzwerk-Logon" anstelle von "Interaktives Logon" verwenden

Diese Einstellung gibt an, wie die Anmeldung mit Benutzername und Kennwort beim Hochladen von Daten auf Netzwerkfreigaben (Schattenkopien, Wiederherstellungsdaten für Bitlocker und Disk Protection) durchgeführt wird.

Für Benutzerkonten aus anderen Domänen oder solche, die nur minimale Rechte haben, um auf den Netzwerkfreigabe zuzugreifen, ist ein interaktiver Logon nicht möglich. Hier funktioniert nur Netzwerk-Logon.

Es ist daher sinnvoll, die Einstellung **Aktiviert** zu verwenden.

5.2.1.6.4 Konfiguration erst aktualisieren, nachdem alle Schutzmechanismen auf dem Agenten aktiv sind

Wenn Sie diese Einstellung aktivieren, startet der DriveLock Agent mit der zuletzt bekannten Konfiguration aus dem Cache. Dies ist dann empfehlenswert, wenn weder das Active Directory noch der DriveLock Enterprise Service (DES) erreichbar sind.

Sie können mit dieser Einstellung

- sicherstellen, dass ein DriveLock Agent die Konfiguration erst dann aktualisiert, sobald alle Schutzmaßnahmen (z.B. Laufwerks- und Applikationskontrolle) aktiviert wurden und
- die Startgeschwindigkeit des Agenten erhöhen.

Hinweis: Diese Einstellung verhindert, dass der Agent mit der aktuellen Richtlinie startet.

5.2.1.6.5 Zugriff auf Agenten außerhalb des Firmennetzwerks ermöglichen (MQTT)

Die Fernsteuerung von Agenten ist bei direktem Netzwerkzugriff immer möglich. Zusätzlich kann durch die Verwendung des MQTT-Protokolls auf Agenten hinter Firewalls oder außerhalb des Firmennetzes zugegriffen werden. MQTT ist standardmäßig aktiviert, aber benötigt auf dem DES CPU und RAM Ressourcen. Daher bietet sich bei einer großen Anzahl von Agenten an, MQTT nicht pauschal für alle Agenten zu aktivieren, sondern nur für solche, die nicht per direktem Netzwerkzugriff zu erreichen sind. Durch die Verwendung von Linked DES Servern kann eine Lastverteilung stattfinden.

5.2.1.7 Einstellungen für die Protokollierung

Mit diesen Einstellungen können Sie zusätzliche Ebenen und Kontexte für die Protokollierung angeben. Diese erlauben eine wesentlich einfachere und schnellere Analyse von Fehlern.

5.2.1.7.1 Protokollierungsgrad

Mit dieser Einstellung können Sie einen festen Wert für den Detaillierungsgrad der Protokolldateien angeben. Zur Wahl stehen 4 Stufen:

- **Fehler**: Nur Fehler werden protokolliert (z.B. Treiber konnte nicht gestartet werden)
- **Info (Standard)**: Nur die wichtigsten Details werden protokolliert. Erlaubt ein 'grobes' Nachvollziehen
- **Detailliert**: Diese Stufe liefert die wichtigsten Informationen
- **Debug**: Diese Stufe liefert eine sehr genaue Fehleranalyse und ist eher selten notwendig. Beachten Sie, dass hierbei die Protokolldatei sehr groß werden kann.

5.2.1.7.2 Maximale Protokolldateigröße in MB

Mit dieser Einstellung können Sie einen maximalen Wert für die Größe der Protokolldatei angeben. Sobald die maximale Größe erreicht ist, wird eine neue Protokolldatei angefangen. Die alte Protokolldatei erhält dann den Namenszusatz 'old', z.B. Drivelock.log wird zu Drivelock.old.log

Der Wert hängt vom Protokollierungsgrad ab.

5.2.1.7.3 Protokollierungskontext

Mit dieser Einstellung können Sie angeben, welcher Prozesse Protokolldateien erstellen.

Werte:

Lokal angemeldeter Benutzer (Standard) und **Remotedesktopverbindung**: Standardmäßig werden hier nur die Prozesse für den lokal angemeldeten Benutzer protokolliert.

> Hinweis: Wenn Sie beispielsweise sämtliche Prozesse auf Terminal Servern protokollieren wollen, insbesondere innerhalb von Benutzer-Sessions, müssen Sie damit rechnen, dass die Anzahl der Protokolldateien enorm ansteigen kann. Daher werden standardmäßig für Benutzer in Remote-Sessions keine Protokolldateien geschrieben.

Normaler Benutzer, **Administrator mit erhöhten Rechten (Standard)** und **Administrator ohne erhöhte Rechte**: Hiermit legen Sie fest, für welche Benutzergruppen die Protokollierung durchgeführt wird. Standardmäßig ist hier immer der Administrator mit erhöhten Rechten gesetzt, damit administrative Tätigkeiten (z.B. für die Problembehebung) immer protokolliert werden.

Prozess: mmc.exe (Standard): Alle Prozesse der DriveLock Management Konsole werden standardmäßig protokolliert.

5.2.1.7.4 Zeit, nach der alte Protokolldateien automatisch gelöscht werden

Mit dieser Einstellung können Sie definieren, nach welcher Zeit alte Protokolldateien automatisch und regelmäßig gelöscht werden.

5.2.2 Einstellungen der Agenten-Benutzeroberfläche

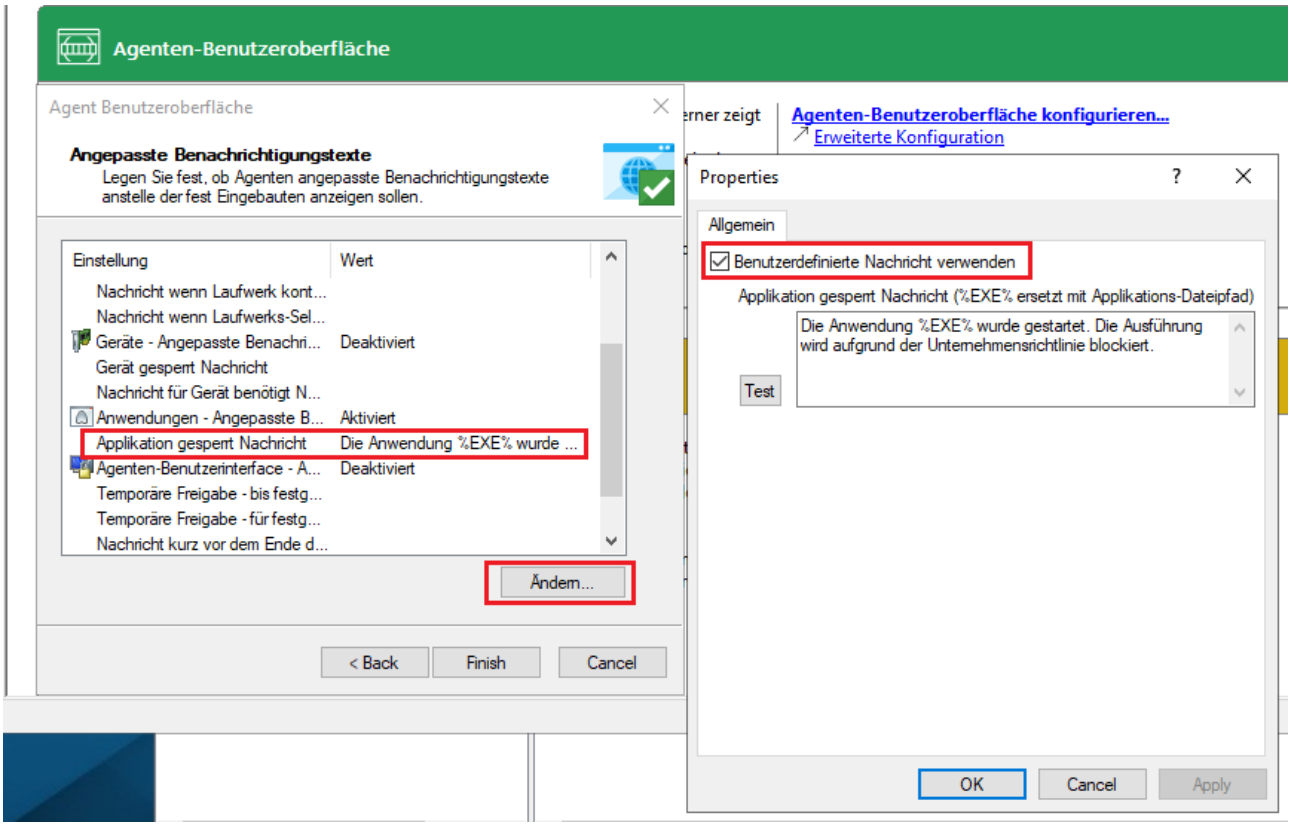
Die Anzeige von Benachrichtigungen beim Endbenutzer kann konfiguriert werden. Wenn Sie die Basis-Einstellungen aktiviert haben, können Sie die Agentenbenachrichtigungen in

einem Assistenten konfigurieren, ansonsten können die Einstellungen über die erweiterte Konfiguration auch einzeln vorgenommen werden.

Im Assistenten geben Sie als erstes die Art der Benachrichtigung an (entspricht der Einstellung für den Taskbar-Informationsbereich). Als nächstes folgen einige Einstellungen für die Offline-Freigabe. Zum Schluss können Sie angepasste Benachrichtigungstexte definieren, falls erforderlich. An dieser Stelle können Sie zentral Texte vorgeben, die dem Endbenutzer in verschiedenen Situationen angezeigt werden. Wenn Sie einen eigenen Text eingeben, zeigt DriveLock diesen anstelle der bereits eingebauten Meldung an.

Für folgende Bereiche können Texte erstellt werden:

- Laufwerkstexte werden angezeigt, wenn DriveLock beispielsweise den Zugriff auf externe Laufwerke oder den Zugriff auf Dateien kontrolliert.
- Gerätetexte werden angezeigt, wenn DriveLock angeschlossene Geräte blockiert.
- Anwendungstexte werden angezeigt, wenn DriveLock den Start von unerlaubten Anwendungen unterbindet.
  In der Abbildung sehen Sie, dass eine benutzerdefinierte Nachricht angezeigt wird, die den Endbenutzer auf das Sperren einer Anwendung hinweist:



5.2.2.1 Einstellungen des Agenten-Benutzerinterface

Mit diesen Einstellungen geben Sie an, welche Funktionen dem Endbenutzer in der Agenten-Benutzeroberfläche zur Verfügung stehen.

Auf dem Reiter **Allgemein** wählen Sie die verschiedenen Kategorien aus, auf dem Reiter **Startmenü** die Stelle im Startmenü, an der DriveLock angezeigt wird. Hier geben Sie auch an, ob eine Verknüpfung zum SB-Freigabe-Assistenten bzw. zur Security-Awareness-Bibliothek im Startmenü des Endbenutzers angezeigt wird.

Informationen zur SB-Freigabe finden Sie hier, zu Security Awareness in der entsprechenden Dokumentation auf DriveLock Online Help.

5.2.2.2 Einstellungen für Taskbar-Informationsbereich

DriveLock kann so konfiguriert werden, dass ein Symbol im Taskbar-Informations-Bereich angezeigt wird und dem Benutzer Benachrichtigungen anzeigt.

Auf dem Reiter **Allgemein** können Sie wählen, ob Benutzerbenachrichtigungen als Popup-Dialogfenster oder Sprechblasentipp beim Beutzer angezeigt werden sollen.

- Wenn Sie **Dialogfenster anzeigen** auswählen, werden konfigurierbare Nachrichten angezeigt. Sie haben auch die Möglichkeit, eigene benutzerdefinierte Nachrichten inklusive HTML-Anweisungen festzulegen.
- Wenn Sie **Sprechblasentipp anzeigen** auswählen, wird die entsprechende Nachricht von Windows als eine Sprechblase angezeigt. Um dies auszuwählen, muss auch die Option **Symbol im Infobereich anzeigen** gesetzt sein.
- Das DriveLock Symbol wird im Informationsbereich benötigt, um Sprechblasen-Tipps anzuzeigen. Sie können das Symbol so konfigurieren, dass es nur während einer Nachricht sichtbar ist. Wählen Sie dazu die Option **Symbol nur anzeigen, wenn Sprechblasentipp aktiv ist**.
- Der **Anzeigedauer**-Balken definiert, wie lange die Nachricht sichtbar ist.
- Um den DriveLock-Ton zu aktivieren, der beim Anzeigen von Nachrichten abgespielt wird, aktivieren Sie die Option **Ton abspielen, wenn eine Nachricht angezeigt wird**.

Auf dem Reiter **Optionen** konfigurieren Sie die Art und Weise, in der DriveLock Funktionen für den Endbenutzer im Kontextmenü des Taskleisten-Symbols angezeigt werden.

- Um die Reihenfolge der Elemente zu ändern, markieren Sie das gewünschte Element und klicken Sie auf **Nach oben** oder **Nach unten**. Klicken Sie **Entfernen**, um das markierte Element zu löschen. Um derzeit nicht sichtbare Elemente wie zum Beispiel eine

Trennlinie hinzuzufügen, klicken Sie auf **Hinzufügen**.

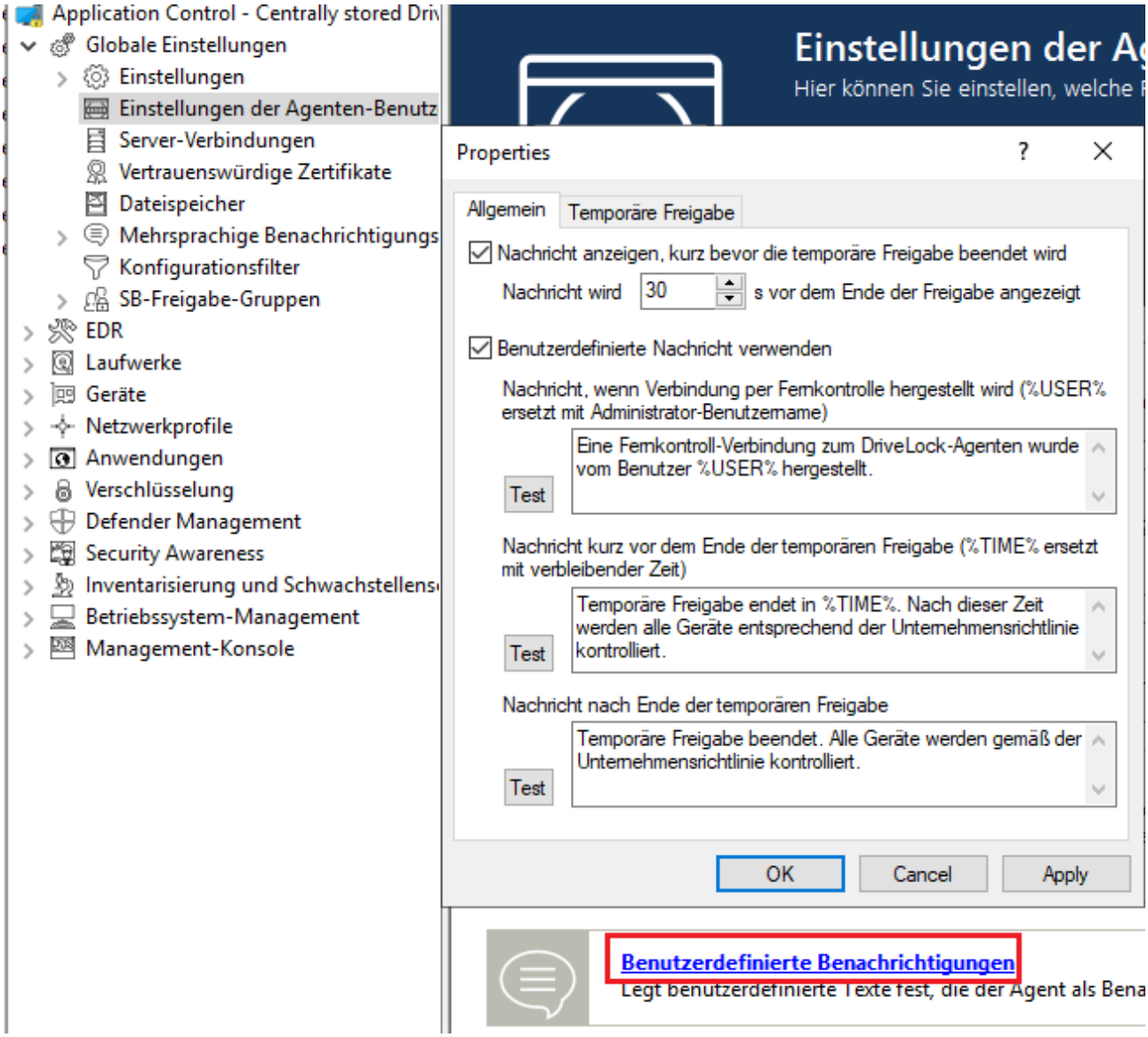
- Um die Standardeinstellungen wiederherzustellen, klicken Sie auf **Zurücksetzen**.

5.2.2.3 Benutzerdefinierte Benachrichtigungen

DriveLock zeigt Benutzer-Benachrichtigungen beim Endbenutzer an, um diesen über Änderungen, beispielsweise Sperrungen oder Freigaben von Geräten oder Laufwerken, zu informieren. Sie können von DriveLock vorgegebene Benachrichtigungen verwenden oder die Texte nach Ihren Vorgaben anpassen. An folgenden Stellen in der DMC können diese Benachrichtigungen angepasst werden:

- Auf der letzten Seite des Assistenten für die Konfiguration der Agenten-Benutzeroberfläche
- In diesem Knoten für die temporäre Freigabe des DriveLock Agenten (s.Abbildung)
- Im Knoten **Mehrsprachige Benachrichtigungen** im Unterknoten **Sprachen / Standard-Nachrichten**. Weitere Informationen finden Sie hier.
- In den **Einstellungen** der Knoten **Laufwerke**, **Geräte** und **Anwendungen** als spezifische Benutzerbenachrichtigungen für diese drei Bereiche.

Auf dem Reiter **Allgemein** können Sie folgende Optionen für die temporäre Freigabe auswählen:



- **Nachricht anzeigen, kurz bevor die temporäre Freigabe beendet wird**: Diese Option ist standardmäßig aktiviert. Bei Bedarf können Sie hier die Zeit einstellen, wann die Benachrichtigung erscheinen soll.
- **Benutzerdefinierte Nachricht verwenden**: Aktivieren Sie diese Option, wenn Sie Ihre eigenen Texte angeben wollen. Folgende Variablen kommend dabei zum Einsatz:
  - `%USER%`: wird beim Anzeigen durch den Benutzernamen des Administrators ersetzt.
  - `%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.

Sie können die Schaltfläche **Test** verwenden, um sich die Nachricht anzeigen zu lassen.

Die Optionen auf dem Reiter **Temporäre Freigabe** sind nur aktiv, wenn Sie benutzerdefinierte Nachrichten verwenden. Hier können Sie Meldungen für die Dauer der kurzzeitige Freigabe anpassen.

> Hinweis: Wenn Sie bereits im Knoten **Mehrsprachige Benachrichtigungen** im Unterknoten **Sprachen / Standard-Nachrichten** eine Sprache festgelegt haben und dort Texte definiert haben, können Sie hier keine Angaben mehr machen.

5.2.2.4 Einstellungen für "Offline-Freigabe"

DriveLock kann gesperrte Wechseldatenträger temporär freigeben, auch wenn der Computer offline ist.

Der dazugehörige Assistent kann mit dieser Einstellung aktiviert oder deaktiviert werden.

Auf dem Reiter **Allgemein** stehen folgende Optionen zur Verfügung:

- Wenn Sie **"Offline Freigabe" deaktivieren** auswählen, kann der Endbenutzer den Assistenten nicht mehr über das Kontextmenü des Taskbarsymbols starten und somit keine Offline-Freigabe mehr anfordern.
- Mit der Option **Kurze (schwache) Anforderungs- und Freigabecodes verwenden** können Sie die Komplexität der Challenge-Response-Codes bei der Offline-Freigabe auf weniger Zeichen reduzieren.

  > Achtung: Durch die Reduzierung der Komplexität wird auch die Sicherheit dieses Verfahrens deutlich reduziert.

- Um die Verwendung des Assistenten komplett zu unterbinden, müssen Sie auch die Option **"Offline Freigabe" im Kontextmenü von DriveLock anzeigen** deaktivieren.
- Sie können einen Mitteilungstext für den Endbenutzer angeben.

Auf dem Reiter **Sicherheit** können Sie festlegen, ob beim Aufruf der Offline-Freigabe eine Authentifizierung durch die Eingabe eines Kennwortes erfolgt oder ob DriveLock mit Hilfe eines Benutzerzertifikates aus dem lokalen Windows-Zertifikatsspeicher den Zugriff auf diese Funktionen freigibt.

- Wählen Sie **Kennwort verwenden**, wenn die Authentifizierung über ein Kennwort durchgeführt werden soll. Geben Sie ein entsprechendes Kennwort ein und bestätigen es.

- Wählen Sie **Zertifikat verwenden**, wenn die Authentifizierung über ein Zertifikat erfolgen soll. Es kann entweder aus einer Datei importiert oder aus dem lokalen Zertifikatsspeicher ausgelesen werden. Sofern Sie die Schaltfläche **Aus Speicher importieren** klicken, werden Sie anschließend aufgefordert, eines der angezeigten Zertifikate auszuwählen.
  Wenn Sie ein Zertifikat verwenden, müssen Sie bei der Genehmigung der Freigabe das Kennwort für den Zugriff auf den privaten Schlüssel des Zertifikates eingeben.

> Hinweis: Die Zertifikate können auch über das DOC importiert werden. Öffnen Sie die Ansicht **Zertifikate** und fügen Sie das entsprechende Zertifikat hinzu. Somit kann die Offline-Freigabe bequem über dieses Zertifikat erfolgen. Ein Kennwort ist nicht mehr erforderlich, allein die Rechte des Benutzers sind ausschlaggebend (d.h. die Rollen für die Zertifikatsverwaltung und für die Offline-Freigabe müssen vergeben sein).

5.2.2.5 Sprache der Agenten-Benutzeroberfläche

Hier stellen Sie die Sprache der DriveLock Agenten ein.

Wenn Sie **Nicht konfiguriert** auswählen, wird die Installation in der Sprache der Windows Installation oder der Spracheinstellung des aktuellen Benutzers stattfinden.

5.2.3 Server-Verbindungen

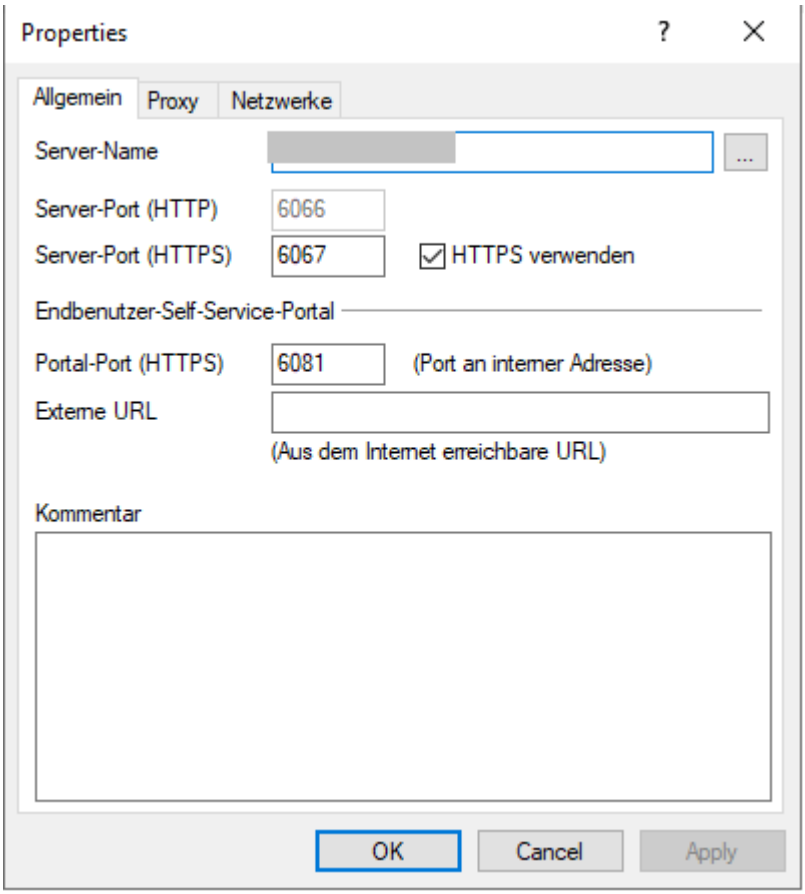
Der DriveLock Enterprise Service (DES) ist die DriveLock Komponente, die alle zentralen Aufgaben und Funktionen durchführt. DriveLock kann mehrere Serververbindungen zu einem DriveLock Enterprise Service verwalten. Verschiedene Verbindungen werden typischerweise in größeren Systemumgebungen oder in Umgebungen mit Außenstandorten verwendet.

Sie können den DES auf einem oder mehreren Computern in Ihrem Netzwerk installieren, allerdings kann es nur eine zentrale DriveLock Datenbank geben.

Unter **Server-Verbindungen** wird Ihnen zunächst nur der DES angezeigt, den Sie bei der Installation konfiguriert haben. Um einen Proxy-Server hinzuzufügen, gehen Sie ebenso vor.

5.2.3.1 Server-Verbindungen konfigurieren

Um eine neue Verbindung hinzuzufügen, rechts-klicken Sie auf **Server-Verbindungen** und wählen anschließend **Neu** und **Server-Verbindung** aus.



Auf dem Reiter **Allgemein** geben Sie den **Server-Name**n an. Sofern Sie bei dessen Installation die Standard-Ports geändert haben, ändern Sie diese hier entsprechend. Standardmäßig verwendet der DriveLock Enterprise Service die Ports 6066 und 6067, um Ereignisse von den Agenten zu erhalten.

- Die Option **HTTPS verwenden** ist standardmäßig ausgewählt. DriveLock erstellt automatisch ein entsprechendes Zertifikat welches für die SSL-Verbindung verwendet wird.
- Wenn Sie das Self-Service-Portal (SSP) verwenden wollen, geben Sie eine **Externe URL** an, über die Endbenutzer das SSP erreichen können. Weitere Informationen zur Konfiguration des SSP finden Sie in der entsprechenden Dokumentation auf DriveLock Online Help.

Auf dem Reiter **Netzwerke** können Sie festlegen, bei welcher Netzwerkverbindung diese Serververbindung verwendet werden soll.

- Die Option **Allen Netzwerken** ist standardmäßig gesetzt und bewirkt, dass die angegebene Serververbindungen unabhängig von der aktuell erkannten Netzwerkverbindung verwendet wird.

- Um eine vorher definierte Netzwerkverbindung anzugeben, aktivieren Sie **Ausgewähltem Netzwerk-Standort** und wählen einen Eintrag aus der Liste aus.
- Wenn die Server-Verbindung verwendet werden soll, wenn sich der Computer an einem bestimmten Active Directory Standort befinden, wählen Sie **Ausgewähltem Active Directory-Standort** und fügen einen Standort hinzu. Dies ist die einfachste Möglichkeit, um für unter-schiedliche Standorte unterschiedliche Server-Verbindungen zu konfigurieren.
- Wenn die Server-Verbindung benutzt werden soll, wenn sich der Computer in einem nicht definierten Netzwerk befindet, aktivieren Sie die Option **Standorten, wo keine andere Verbindung konfiguriert ist**.

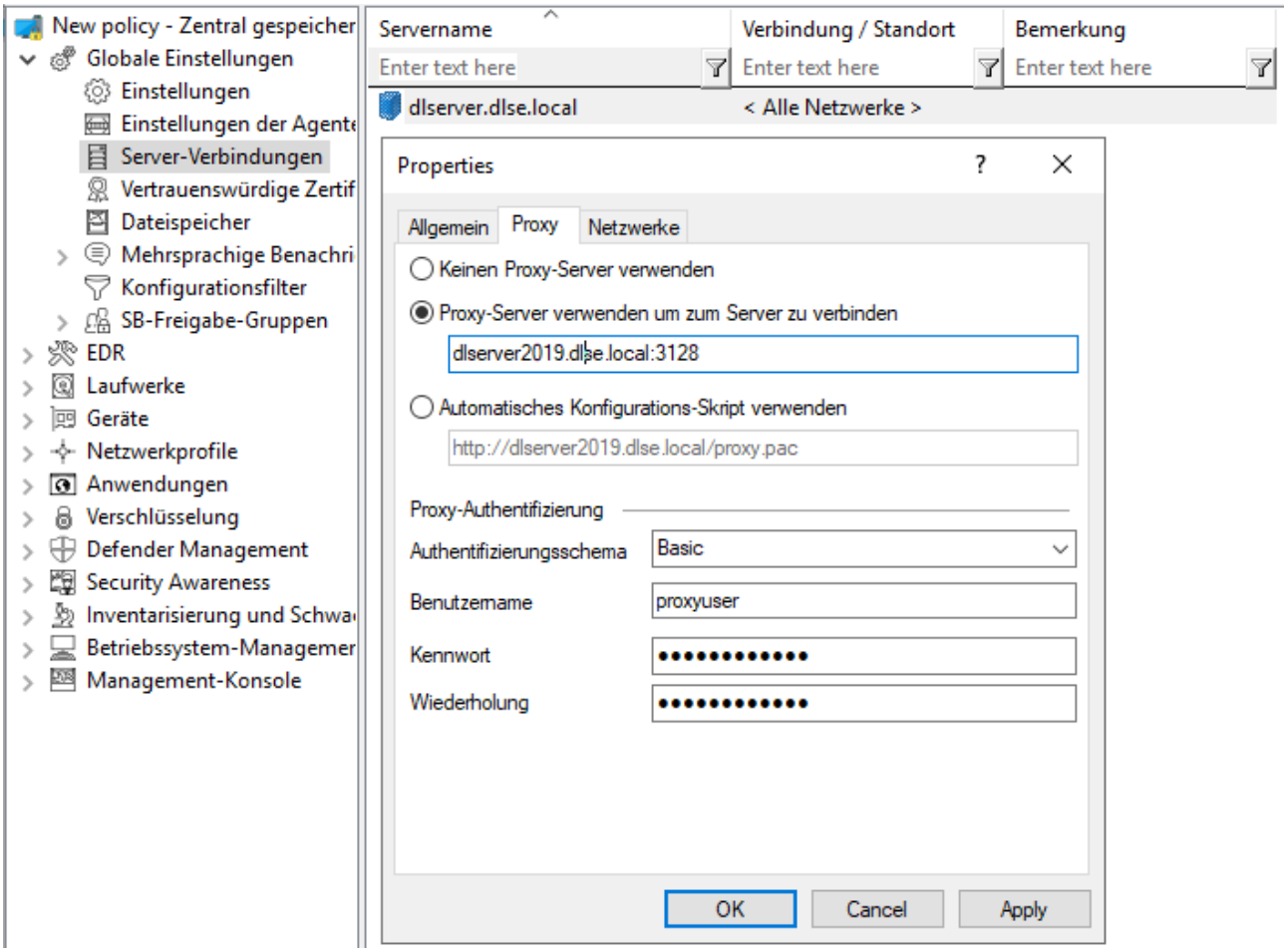
Der Reiter **Proxy** ist hier beschrieben.

5.2.3.2 Proxy-Server

Sie können bei den DES-Verbindungseinstellungen einen Proxy-Server angeben. Es ist möglich, pro Server jeweils einen anderen Proxy anzugeben.

Auf dem Reiter **Proxy** wählen Sie die Option **Proxy-Server verwenden, um zum Server zu verbinden** und geben den entsprechenden Server an.

Alternativ können Sie auch ein **Automatisches Konfigurations-Skript verwenden** (*.pac-Datei). Geben Sie dazu die URL entsprechend an. Geben Sie ggf. das Authentifizierungsschema, einen Benutzernamen und Kennwort ein.



Achtung: Sobald Sie einen Proxy-Server in der Richtlinie angeben, werden evtl. bei der Installation gesetzte Einstellungen nicht mehr verwendet.

Informationen zu Proxy-Einstellungen auf dem DriveLock Agenten finden Sie hier.

5.2.4 Vertrauenswürdige Zertifikate

DriveLock verwendet vertrauenswürdige Zertifikate für die sichere Kommunikation zwischen der DriveLock Management Konsole bzw. den DriveLock Agenten und dem DES eingeführt. Sie können diese Zertifikate in den Globalen Einstellungen einer Richtlinie angeben.

Hinweis: Seit Version 2019.2 befindet sich das Tool **ChangeDesCert.exe** im Programmverzeichnis des DriveLock Enterprise Services (DES) unter C:\Program Files\CenterTools\DriveLock Enterprise Service\ChangeDesCert.exe.
Beachten Sie dazu folgendes: Wenn Sie ein vorhandenes DES-Server-Zertifikat mit dem Tool austauschen möchten, muss das neue Zertifikat in den Computer-Zertifikatspeicher importiert und der private Schlüssel als exportierbar konfiguriert werden.

Wichtige Informationen:

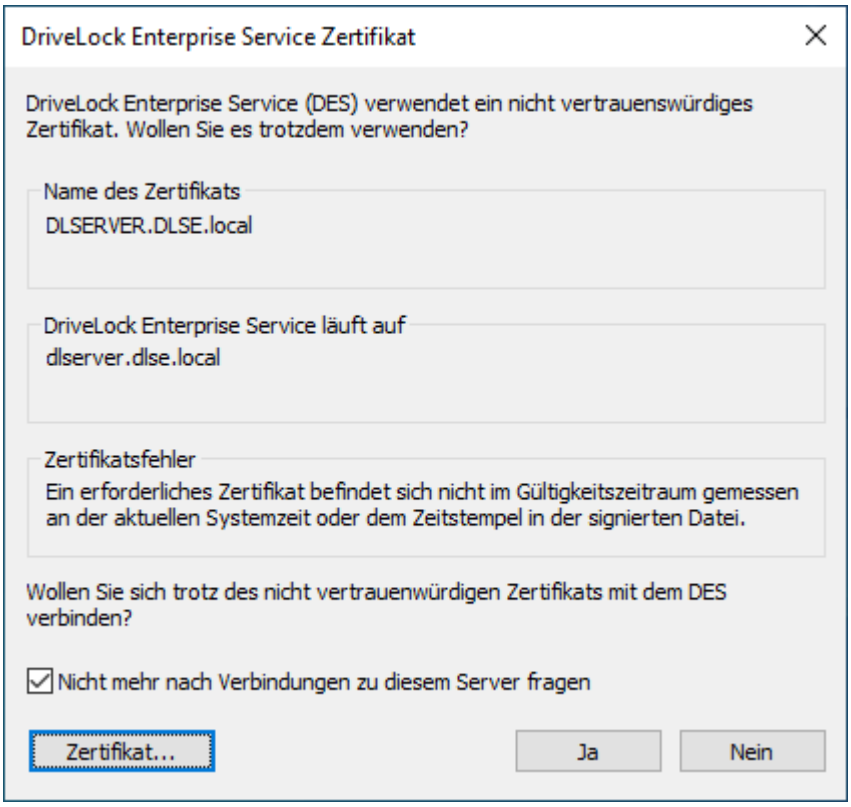
- Sorgen Sie dafür, dass Ihre Zertifikate immer auf dem aktuellen Stand sind. Wenn Sie das DES Zertifikat aus-tauschen müssen oder weitere verknüpfte DES installiert haben, tragen Sie bitte rechtzeitig die neuen Zertifikate in die Liste ein und stellen Sie sicher, dass die DriveLock Agenten diese Richtlinie zugewiesen bekommen, bevor sie mit dem DES (oder dem neuen verknüpften DES) kommunizieren.
- Solange es einem DriveLock Agenten noch nicht gelungen ist, das DES Zertifikat in der Liste der vertrauenswürdigen Zertifikate zu finden, akzeptiert er Verbindungen zu jedem DES. Sobald das Zertifikat einmal erfolgreich geprüft ist, kommuniziert der Agent ab diesem Moment nur noch mit den DES, deren Hashwerte in der Liste der vertrauenswürdigen Zertifikate eingetragen sind.
- Wenn Sie alle Zertifikate aus dieser Liste entfernen, kommunizieren die Agenten wieder mit allen DES.

Hinweis: Wenn ein DriveLock Agent ein ungültiges Zertifikat erhält, wird eine Fehlermeldung auf dem Agenten angezeigt und es findet keinerlei Kommunikation mehr zwischen DES und Agent statt! In diesem Fall sind manuelle Änderungen in der lokalen Registry des Agenten die einzige Lösung. Bitte kontaktieren Sie den DriveLock Support für weitere Informationen.

5.2.4.1 Vertrauenswürdige Zertifikate in der DMC prüfen

Bei jedem Aufruf einer DriveLock Enterprise Service Funktion prüft die DriveLock Management Konsole (DMC) das Zertifikat, das der Server verwendet.

Wenn Windows das Zertifikat als nicht vertrauenswürdig einstuft oder das Zertifikat ungültig ist, erscheint zunächst folgende Meldung (siehe Abbildung).



Achtung: Bitte beachten Sie, dass selbstsignierte Zertifikate von Windows zunächst als nicht vertrauenswürdig eingestuft werden, weil das Root-Zertifikat nicht überprüft werden kann.

Sie können sich das Zertifikat ansehen und nachprüfen, dass es sich tatsächlich um das Zertifikat handelt, das der DES verwendet, bevor Sie der Verwendung zustimmen. In diesem Fall wird in der Registry ein entsprechender Eintrag unter `HKEY_CURRENT_USER/SOFTWARE/CenterTools/DriveLock/MMC` vorgenommen. Die Meldung erscheint danach nicht mehr, weil somit das Zertifikat eingetragen ist.

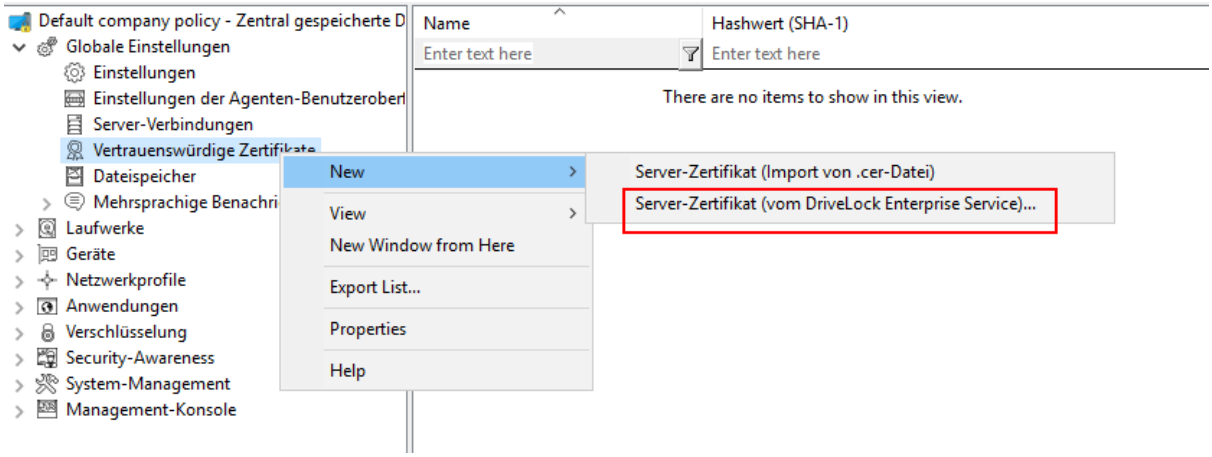
5.2.4.2 Vertrauenswürdige Zertifikate auswählen

Hinweis: Wir empfehlen diese Einstellung zu nutzen, um die Sicherheitsvoraussetzungen für die Kommunikation zwischen DriveLock Agent und DriveLock Enterprise Service zu erhöhen. Wenn Sie keine Zertifikate angeben, kann DriveLock nicht sicherstellen, dass der Agent mit dem richtigen DES kommuniziert.

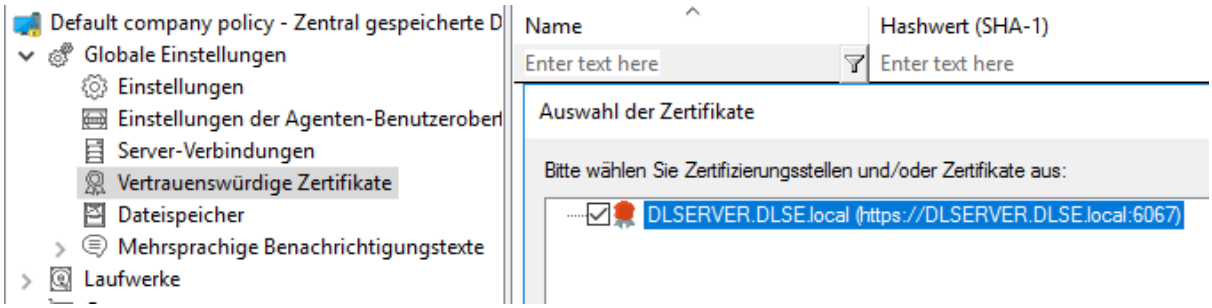
Weitere Informationen zu Zertifikaten finden Sie im Installationshandbuch auf DriveLock Online Help. Wenn Sie selbstsignierte Zertifikate verwenden, sollten Sie diese unbedingt angeben. Zertifikate, die von einer Zertifizierungsstelle (CA) ausgestellt werden, können von Windows überprüft werden.

Bei der Auswahl der vertrauenswürdigen Zertifikate gibt es zwei Möglichkeiten:

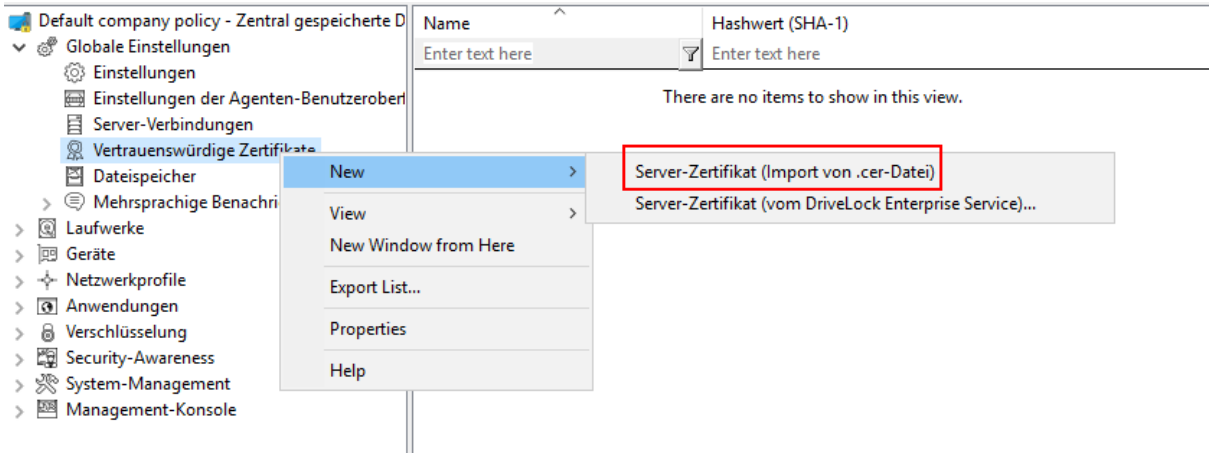
1. Wenn Sie das Server-Zertifikat verwenden, das Sie während der Installation des DES mit der Option **Create self-signed certificate** gewählt haben, wählen Sie hier im Kontextmenü **Neu** und dann **Server-Zertifikat (vom DriveLock Enterprise Service)**. Sie können direkt das Zertifikat auswählen, das vom DES (oder verknüpftem DES) verwendet wird (siehe Abbildung).



Danach setzen Sie ein Häkchen bei denjenigen DES (bzw. verknüpften DES) Zertifikaten, mit denen der Agent kommuniziert (im Beispiel unten DLSERVER.DLSE.local...):



2. Wenn Sie ein eigenes Server-Zertifikat für die Kommunikation angegeben haben, können Sie dieses hier auswählen und in Ihrer Richtlinie verwenden:



Wählen Sie im nächsten Schritt das entsprechende Zertifikat in der Verzeichnisstruktur aus.
Sie können bei dieser Option auch das Root-CA-Zertifikat importieren. Damit erreichen Sie, dass DriveLock Agenten allen Zertifikaten mit dieser Root-CA vertrauen. Wenn Ihre DES Zertifikate dieselbe Root-CA haben, müssen Sie diese nicht mehr einzeln auflisten.
In der Liste der vertrauenswürdigen Zertifikate wird nun die entsprechende Information zum Zertifikat angezeigt (z.B. Name und Hashwerte SHA-1 und SHA-256).

Hinweis: Anmerkung: Der Hashwert SHA-1 wird nur noch für XP verwendet.

Die DriveLock Agenten, auf die Sie Ihre Richtlinie dann zuweisen, werden das Server-Zertifikat als vertrauenswürdig einstufen und nur mit den entsprechenden vertrauenswürdigen Servern kommunizieren.

5.2.5 Dateispeicher

Der DriveLock Richtliniendateispeicher ist ein geschützter Speicherbereich innerhalb einer DriveLock Richtlinie. Er wird beispielsweise dazu verwendet, um Dateien zu speichern, die über einen Kommandozeilenbefehl innerhalb einer DriveLock Whitelist-Regel ausgeführt werden sollen. Der Richtliniendateispeicher vereinfacht somit die Verteilung von Skripten oder Programmen, die vom DriveLock Agenten auf Client Computern verwendet werden. Nachdem Sie Dateien in den Richtliniendateispeicher importiert haben, werden diese zusammen mit den anderen Einstellungen automatisch an die Agenten verteilt. Sie können den Richtliniendateispeicher in einer lokalen Richtlinie ebenso verwenden, wie innerhalb einer Konfigurationsdatei oder einer Gruppenrichtlinie.

Achtung: Der Import großer Dateien in den Richtliniendateispeicher kann den Netzwerkverkehr erhöhen und die Anmeldezeiten von Benutzern verlängern, da der Computer diese Dateien erhält, wenn die Gruppenrichtlinien auf einen Computer angewendet werden und der Speicher entweder noch nicht geladen wurde oder sich geändert hat.

Klicken Sie auf Datenspeicher, um eine Liste mit allen im Richtliniendateispeicher enthaltenen Dateien zu sehen.

Rechts-klicken Sie auf **Dateispeicher** und wählen anschließend **Neu** und dann **Datei...**, um eine Datei in den Richtliniendateispeicher zu importieren. Wählen Sie die gewünschte Datei mit Hilfe des Dateiauswahldialoges aus.

Rechts-klicken Sie auf eine Datei und wählen aus den folgenden Möglichkeiten:

- **Datei extrahieren**: Speichern sie eine Kopie der Datei in einem beliebigen Ordner.
- **Löschen**: Löschen Sie die angewählte Datei aus dem Richtliniendateispeicher.
- **Eigenschaften**: Lassen Sie sich Details zur ausgewählten Datei anzeigen.

Rechts-klicken Sie auf **Dateispeicher** und wählen Sie die Option **Systemdaten anzeigen**, um auch die Dateien zu sehen, die von DriveLock intern innerhalb des Richtliniendateispeichers abgelegt werden (wie zum Beispiel die Recovery-Zertifikate oder Anwendungs-Hash-Datenbanken).

Hinweis: Systemdateien können nicht aus dem Richtliniendateispeicher gelöscht werden.

Rechts-klicken Sie auf **Dateispeicher** und wählen **Eigenschaften**, um weitere Informationen über den Richtliniendateispeicher zu erhalten.

Um einen neuen Richtliniendateispeicher zu erstellen, klicken Sie auf **Speicher zurücksetzen**.

Achtung: Das Zurücksetzen des Richtliniendateispeichers hat zur Folge, dass alle enthaltenen Dateien inklusive der Systemdateien gelöscht werden. Stellen Sie unbedingt sicher, dass Sie eine Kopie der Dateien haben, bevor Sie den Richtliniendateispeicher löschen, insbesondere wenn Sie die DriveLock Disk Protection verwenden.

5.2.6 Mehrsprachige Benachrichtigungstexte

Sie können innerhalb von DriveLock einzelne Textmeldungen in unterschiedlichen Sprachen erstellen, die bei verschiedenen Benutzerbenachrichtigungen verwendet werden können.

Bevor Sie einzelne Textmeldungen in Whitelist-Regeln verwenden können, müssen zunächst die Sprachen, die verfügbar sein sollen, festlegen.

5.2.6.1 Sprachen / Standard-Nachrichten

Rechts-klicken Sie auf **Sprachen / Standard-Nachrichten**, dann **Neu** und wählen zunächst auf dem Reiter **Allgemein** die gewünschte **Sprache** aus. Die Liste enthält alle derzeit verfügbaren Windows-Sprachen. Sie können optional auch eine Beschreibung hinzufügen.

Für folgende Bereiche können Benachrichtigungen definiert werden:

Wählen Sie den Reiter **Laufwerkskontrolle** und geben Sie die Standardmeldungen ein, die DriveLock beim Sperren von Laufwerken verwenden soll.

- 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 Meldungen für den Zugriff auf Dateien oder z.B. 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.

Wählen Sie den Reiter **Geräte**, um die Standard-Meldungen für Geräte festzulegen. Die Variable `%DEV%` wird beim Anzeigen durch den aktuellen Gerätenamen ersetzt.

Auf dem Reiter **Applikationen** können die Meldungen für die Applikationskontrolle definiert werden.

- Die Variable `%EXE%` wird beim Anzeigen durch die aktuelle Anwendung ersetzt.
- Die Variable `%PARENT%` wird ersetzt für den Programmstart.

Auf dem Reiter **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.
- Sie sollten einen Informationstext konfigurieren, der auf der ersten Seite des Freigabeassistenten angezeigt wird.

Auf dem Reiter **Verwendungsrichtlinie** definieren Sie die Texte für Verwendungsrichtlinien.

- Verwendungsrichtlinien dienen dazu, den Benutzer vor dem eigentlichen Zugriff auf ein Laufwerk oder ein Gerät über sicherheitsrelevante Verhaltensmaßnahmen oder Unternehmensrichtlinien zu informieren. Erst nachdem der Benutzer eine Hinweismeldung (Verwendungsrichtlinie) gelesen und nachvollziehbar akzeptiert hat,

wird das Laufwerk oder Gerät freigegeben.

- Sowohl eine Überschrift, die Texte für die beiden Schaltflächen, als auch der Text selbst kann dabei frei über diesen Konfigurationspunkt definiert werden.
- Geben Sie den Nachrichtentext entweder direkt in das Eingabefeld ein, oder wählen Sie eine RTF-formatierte Datei von der lokalen Festplatte bzw. aus dem Richtlinienspeicher aus. Eine Datei aus dem Richtlinienspeicher ist mit einem „*“ markiert.

> Achtung: Wenn Sie eine Datei auswählen, müssen Sie sicherstellen, dass diese sich im angegebenen Pfad auf der lokalen Festplatte des Client-Rechners befindet und von dort geladen werden kann. Über den Richtlinienspeicher können Sie diese Datei zusammen mit der DriveLock Konfiguration verteilen. Mehr zum Thema Richtlinienspeicher finden Sie unter Dateispeicher.

- Innerhalb der Verwendungsrichtlinie lässt sich auch ein AVI-Video abspielen, welches ebenfalls über diesen Dialog konfiguriert werden kann.

Auf dem Reiter **Agent** können Sie die Meldung für den Fernkontrollzugriff konfigurieren.

- Sie können einen Informationstext konfigurieren, der dem angemeldeten Benutzer angezeigt wird, sobald ein Administrator eine Fernkontrollverbindung aufbaut.
- Die Variable `%USER%` wird beim Anzeigen durch den Benutzernamen des Administrators ersetzt, welcher den Fernkontrollzugang gestartet hat.

Auf dem Reiter **Awareness** legen Sie die Standardtexte für das Anzeigefenster der Security Awareness Kampagnen fest.

Auf dem Reiter **Verschlüsselung** geben Sie einen Kontakt an (z.B. den Administrator oder HelpDesk), an den sich der Endbenutzer wenden kann, um den Wiederherstellungsprozess durchführen zu können.

5.2.6.2 Benachrichtigungstexte

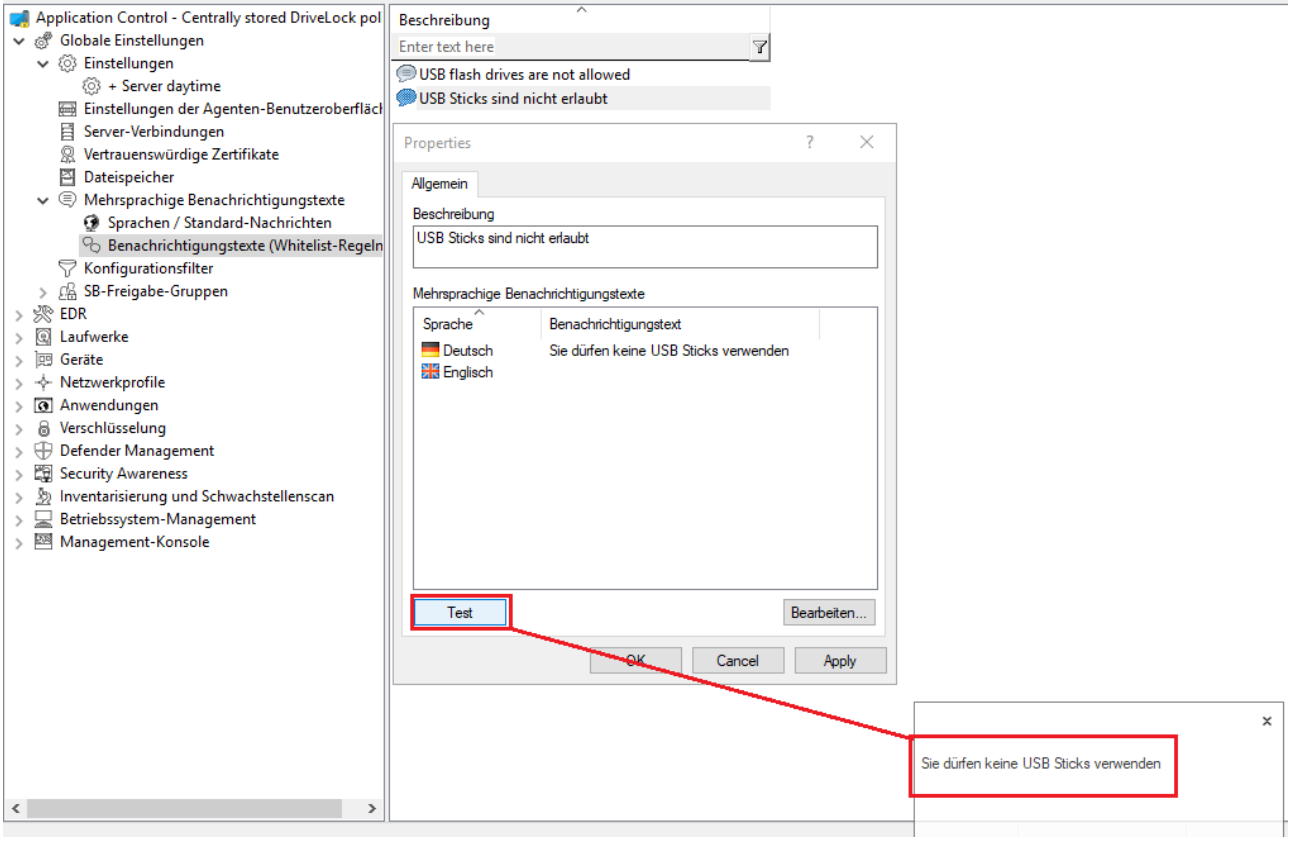
Hier können Sie einzelne Benutzermeldungen für verschiedene Sprachen erstellen. Zusätzlich zu den Standardmeldungen können weitere Benutzerbenachrichtigungen definiert und innerhalb von Whitelist-Regeln verwendet werden. Zuvor müssen aber – wie im vorhergehenden Abschnitt beschrieben – die zur Verfügung stehenden Sprachen konfiguriert werden.

Rechts-klicken Sie **Benachrichtigungstexte (Whitelist-Regeln)**, dann Neu und **Benachrichtigungstext**.

Geben Sie einen beschreibenden Text ein. Dieser wird auch in der Liste angezeigt, aus der Sie innerhalb von Whitelist-Regeln eine spezielle Benachrichtigung auswählen können.

Alle verfügbaren Sprachen werden angezeigt. Um eine Nachricht in einer dieser Sprachen zu verfassen, wählen Sie die Sprache aus und klicken auf **Bearbeiten**.

Verwenden Sie nach der Eingabe des Textes die Schaltfläche **Test**, um zu prüfen ob die Meldung korrekt angezeigt wird. Klicken Sie OK, um den eingegebenen Text zu übernehmen.



Wiederholen Sie diese Schritte, um für alle Sprachen den jeweiligen Text einzugeben.

> Hinweis: Die Verwendung von mehrsprachigen Meldungen wird innerhalb der jeweiligen Whitelist-Regeln definiert.

5.2.7 Konfigurationsfilter

Ausgangslage:

Grundsätzlich gilt eine Einstellung überall, wo die entsprechende Richtlinie auch gilt. Eine spezifische Einstellung wird also in einer spezifischen Richtlinie gesetzt. Wenn man demnach einzelne Einstellungen unterschiedlich setzen wollte, müsste man eine zweite Richtlinie erstellen.

Mit Hilfe von Konfigurationsfiltern für unterschiedliche Computer, Benutzer oder Zeiten innerhalb einer einzigen Richtlinie erspart man sich das Erstellen einer neuen Richtlinie und somit den Aufwand, eine große Menge an Richtlinien mit Einzeleinstellungen pflegen zu müssen.

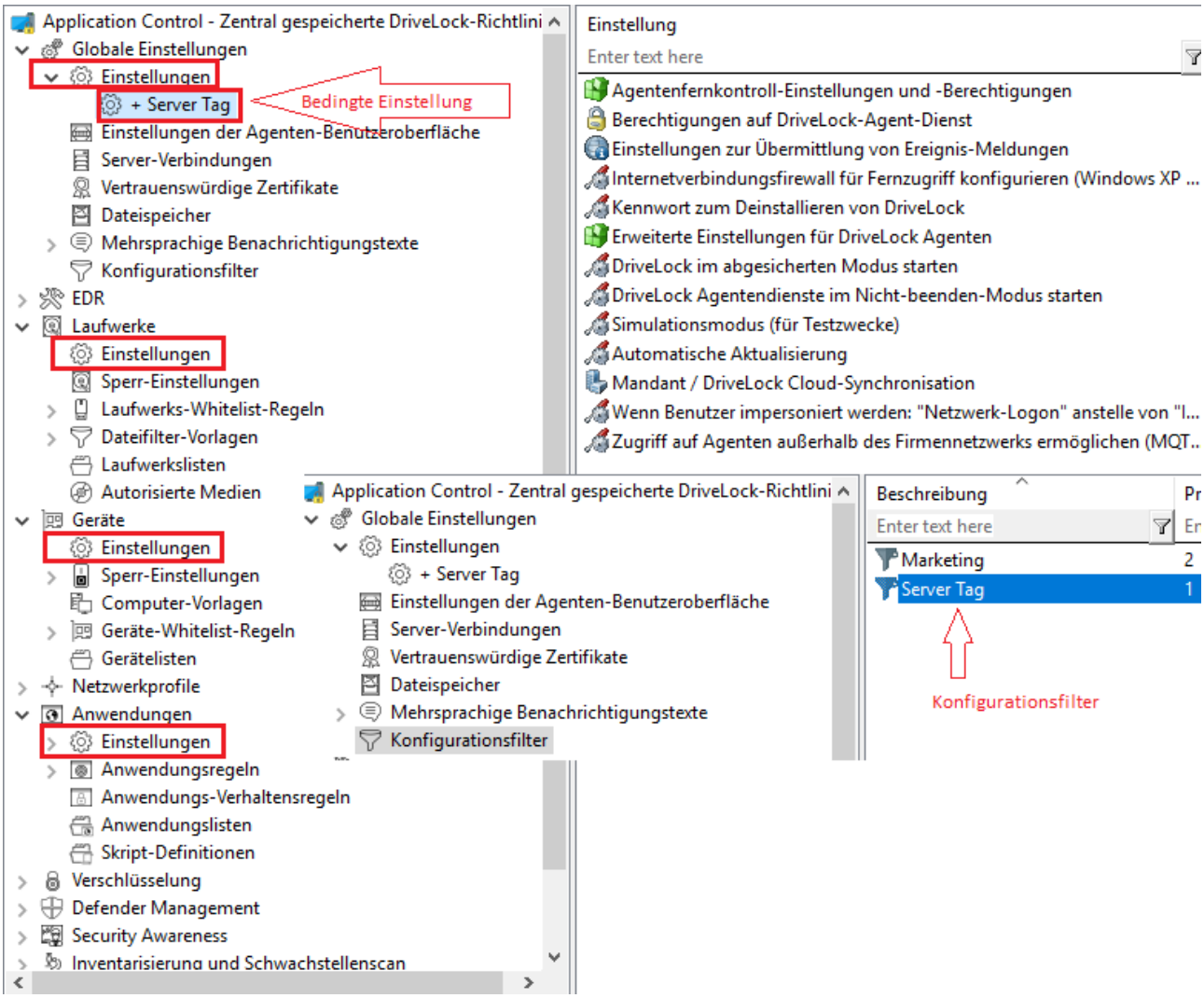
Wirkung:

Mit Konfigurationsfiltern können Sie Bedingungen (d.h. "bedingten Einstellungen") für bestimmte Computer, Benutzer oder Zeiten in einer einzigen Richtlinie kombinieren. Der Konfigurationsfilter allein hat keine Funktionalität, sondern wird als Kriterium für bedingte Einstellungen verwendet. Er kann in sämtlichen Einstellungsknoten der DriveLock Management Konsole verwendet werden.

Hier sehen Sie, wie Sie einen Konfigurationsfilter anlegen und als bedingte Einstellung verwenden.

Verwendung des Konfigurationsfilters in bedingten Einstellungen:

Unterhalb der verschiedenen Einstellungsknoten werden Duplikate des jeweiligen Knotens erstellt, die mit einem Konfigurationsfilter verknüpft sind.



In diesem Knoten gesetzte Einstellungen greifen nur, wenn der Filter auf den Reitern Computer, Benutzer oder Zeiten erfüllt ist.

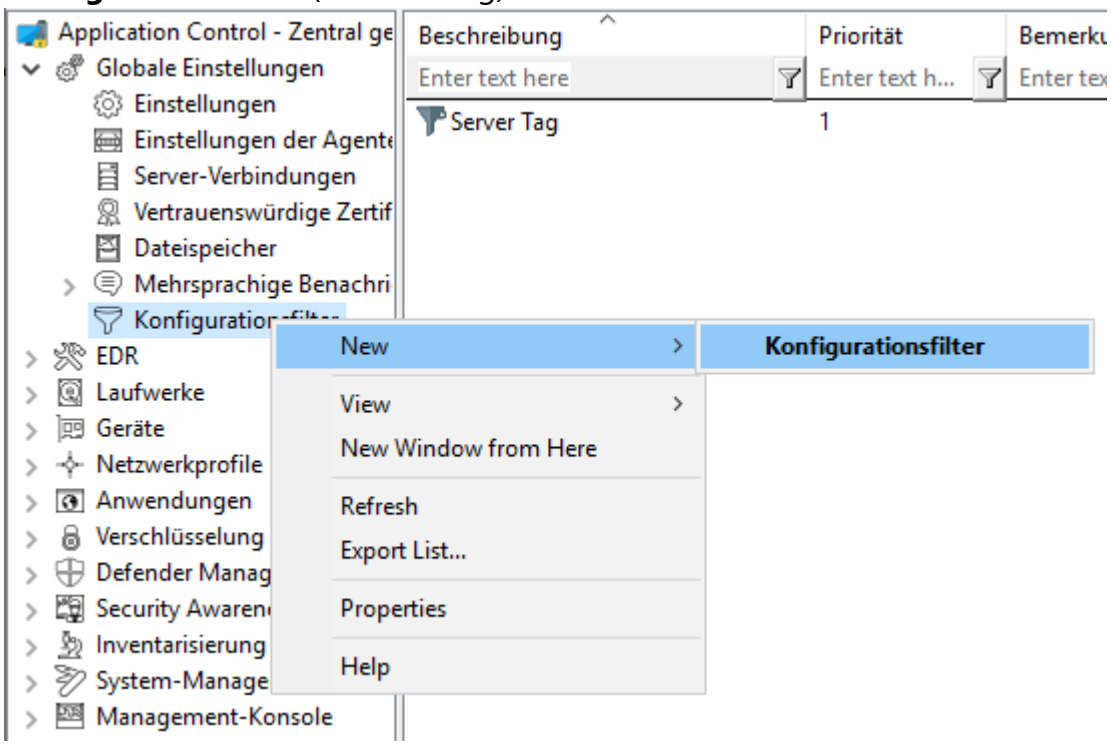
Vorteile von bedingten Einstellungen:

- Es stehen Ihnen mehr Einstellmöglichkeiten als in einer normalen Richtlinie zur Verfügung (weil Sie z.B. aktive Zeiten für die Bedingungen einstellen können)
- Sie sparen sich die Erstellung vieler Richtlinien und deren Zuweisungen
- Einzelne Einstellungen können leichter überschrieben werden
- Sie können Ihre Einstellungen leichter nachvollziehen, weil alles in einer einzigen Richtlinie enthalten ist
- Konfigurationsfilter greifen auch offline

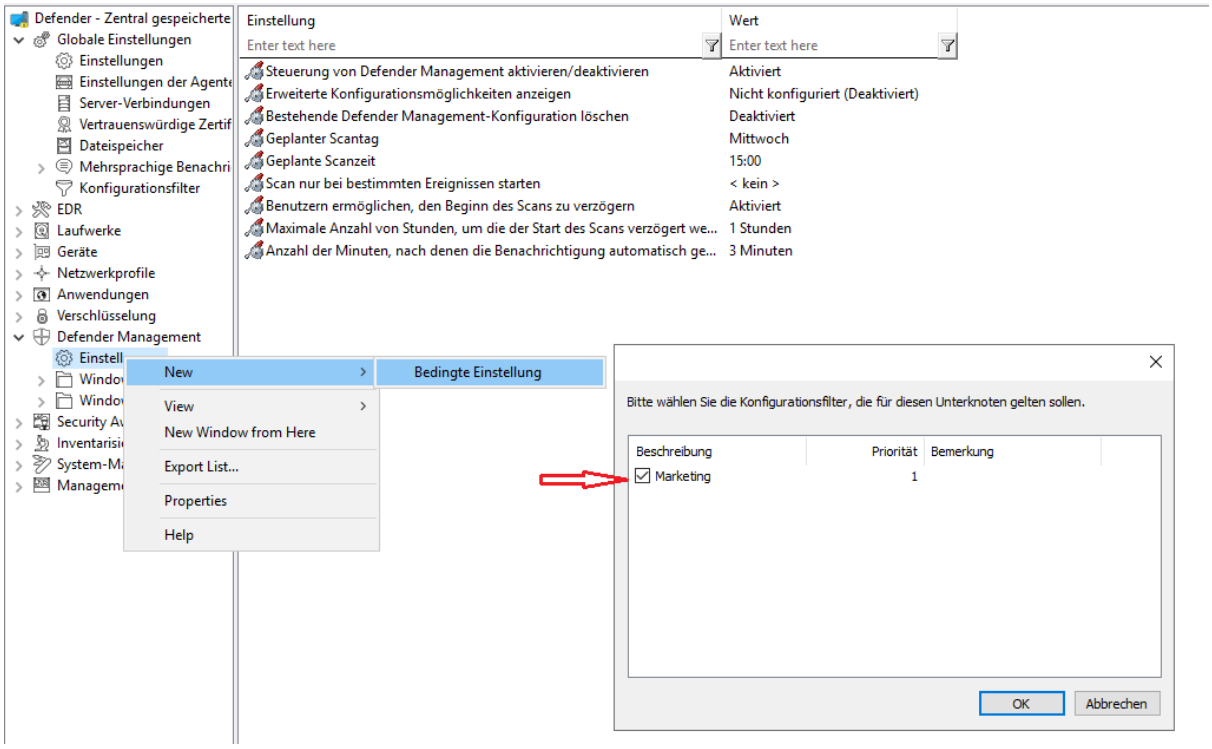
5.2.7.1 Konfigurationsfilter anlegen und bedingte Einstellung setzen

Legen Sie Konfigurationsfilter folgendermaßen an:

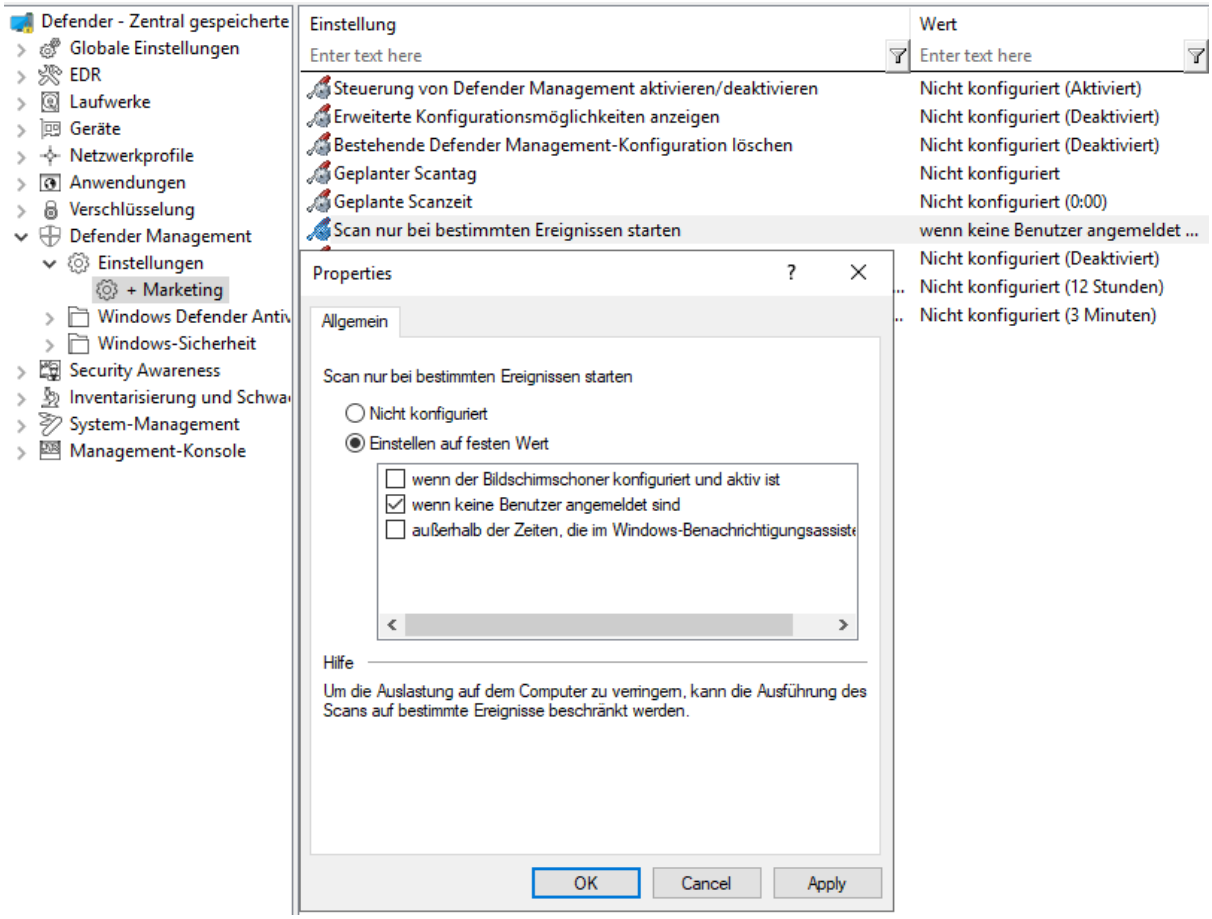
1. Öffnen Sie im Knoten **Konfigurationsfilter** das Kontextmenü **Neu**/New und dann **Konfigurationsfilter** (s. Abbildung).



2. In den Eigenschaften des Konfigurationsfilters geben Sie eine Beschreibung und ggf. einen Kommentar ein. Im Beispiel unten heißt der Konfigurationsfilter **Marketing**.
3. Je nachdem, welche Bedingungen Sie setzen wollen (bestimmte **Zeiten**, **Computer** oder **Angemeldete Benutzer**), geben Sie auf den entsprechenden Reitern die gewünschten Einstellungen an. Ein Anwendungsbeispiel finden Sie hier.
4. Speichern Sie den Konfigurationsfilter ab.
5. Als nächstes setzen Sie den Konfigurationsfilter als bedingte Einstellung in einem beliebigen Einstellungsknoten der DriveLock Management Konsole ein.
   Beispiel:
   Wenn Sie die Einstellungen von Defender Management mit einer Bedingung für bestimmte Client-Computer verknüpfen wollen (im Beispiel die Computer der Abteilung Marketing), gehen Sie wie in der Abbildung gezeigt vor:



6. Dann wählen Sie die Einstellung, die explizit für die Marketing-Computer gelten soll. Im Beispiel soll der Defender Scan bei den Marketing-Computern nur gestartet werden, wenn keine Benutzer angemeldet sind:



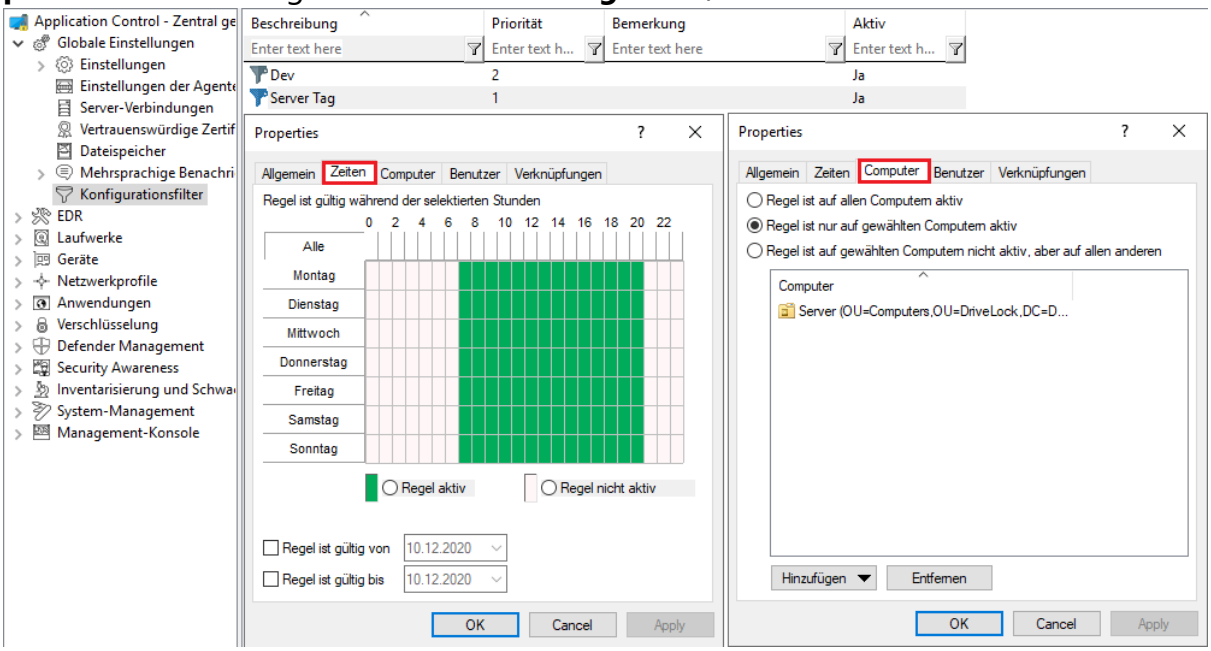
7. Speichern Sie Ihre Einstellung und weisen Sie dann die Richtlinie zu.

5.2.7.2 Anwendungsfall für Konfigurationsfilter

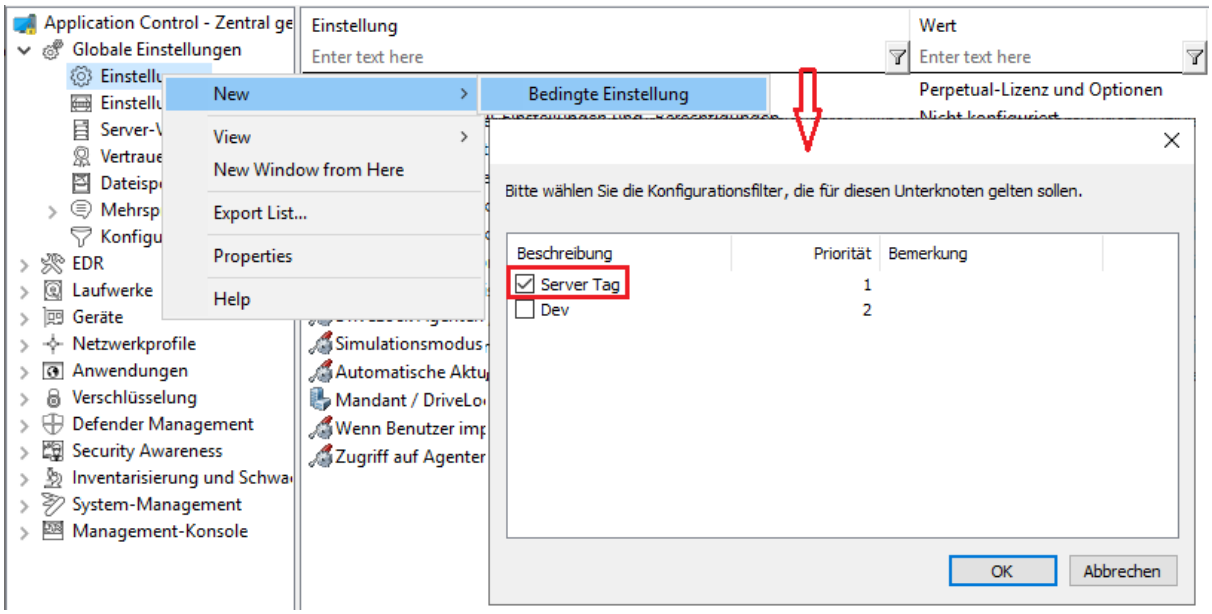
Ziel: Sie wollen für bestimmte DriveLock Agenten (Server) die automatische Aktualisierung tagsüber abschalten.

Gehen Sie folgendermaßen vor:

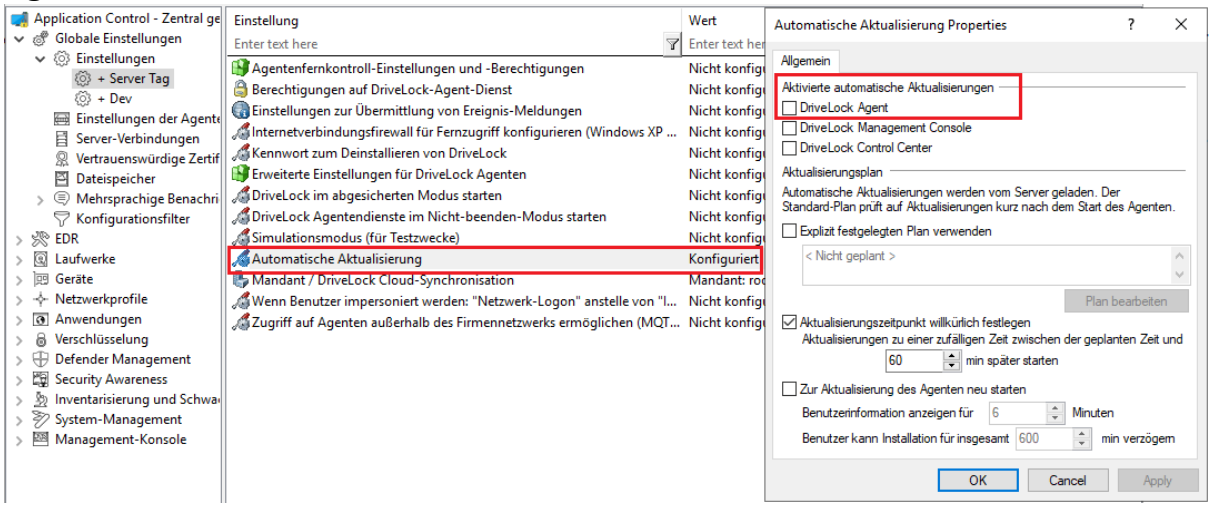
1. Legen Sie einen neuen Konfigurationsfilter an.
2. Geben Sie im Dialog eine **Beschreibung** (Beispiel Server Tag) und einen **Kommentar** ein. Das Häkchen bei **Ist aktiv** ist standardmäßig gesetzt.
3. Wählen Sie auf dem Reiter **Zeiten** aus, wann die Regel aktiv sein soll (tagsüber).
4. Wählen Sie auf dem Reiter **Computer** die Option **Regel ist nur auf gewählten Computern aktiv** und fügen Sie unter **Hinzufügen** die/den Server Ihrer Wahl aus.



5. Speichern Sie den Konfigurationsfilter ab.
6. Der angelegte Konfigurationsfilter erscheint nun im gleichnamigen Knoten und kann als bedingte Einstellung verwendet werden.
7. Hierzu wählen Sie unter **Globale Einstellungen** den Unterknoten **Einstellungen**, öffnen das Kontextmenü und wählen New/**Neu** und als Bedingte Einstellung Ihren Konfigurationsfilter **Server Tag**.



8. Öffnen Sie dann in dieser bedingten Einstellung die Option **Automatische Aktualisierung** und entfernen Sie das standardmäßig gesetzte Häkchen bei **DriveLock Agent**.



9. Speichern Sie Ihre Konfiguration ab.

Fazit:

Die Regel mit der bedingten Einstellung 'Automatische Aktualisierung' ist somit auf den definierten Servern tagsüber abgeschaltet, auf allen anderen DriveLock Agenten aber aktiv (wie in den normalen Einstellungen gesetzt).

Begründung:

Bedingte Einstellungen überschreiben die normalen Einstellungen

Hinweis: Wenn es mehrere bedingte Einstellungen gibt, hängt es von der Priorität der Konfigurationsfilter ab, wann sie angewendet werden. Sie können die Priorität anpassen.

5.2.8 SB-Freigabe-Gruppen

Mit Hilfe von SB-Freigabe-Gruppen können Sie autorisierten Benutzern erlauben, DriveLock Agenten selbst freizugeben, ohne die DriveLock Management Console (MMC) oder das DriveLock Operations Center (DOC) benutzen zu müssen.

Die Prinzipien der Freigabe von Agenten sind hier erläutert.

5.2.8.1 Einstellungen

Die drei Einstellungen für die SB-Freigabe werden verwendet, damit Endbenutzer diese Funktionalität auch dann verwenden dürfen, wenn ihre Computer entweder in keiner oder in einer anderen Domäne sind.

In diesen Fällen können Sie ein Konto (oder auch ein alternatives Konto) angeben, damit Active Directory-Abfragen durchgeführt werden können.

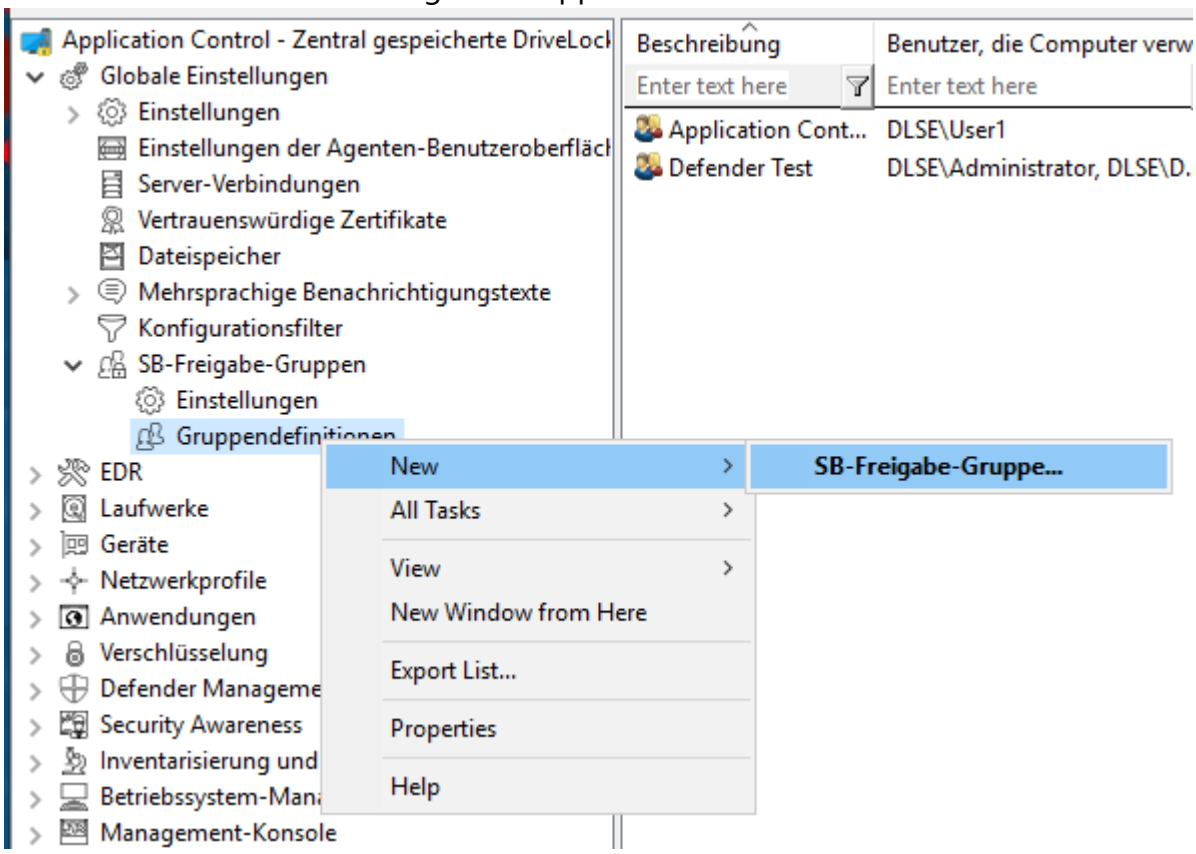
Mit Hilfe der Einstellung **"Ausführen als"-Seite am Beginn des Freigabeassistenten anzeigen** bekommt der Benutzer bei Beginn des SB-Freigabeassistenten die Möglichkeit ein anderes Konto für die Anmeldung zu verwenden.

5.2.8.2 Gruppendefinitionen

Damit Benutzer die SB-Freigabe verwenden dürfen, müssen sie in eine SB-Freigabe-Gruppe aufgenommen werden. Hier geben Sie die Module an, die Sie für die SB-Freigabe erlauben wollen (z.B. nur Laufwerke oder nur Anwendungen).

Gehen Sie folgendermaßen vor:

1. Erstellen Sie eine neue SB-Freigabe-Gruppe.



2. Auf dem Reiter **Allgemein** geben Sie eine kurze Beschreibung und einen Kommentar an, um diese SB-Freigabe-Gruppe zu identifizieren. Nutzen Sie das Feld **End-benutzerinformation** für eine Erklärung wann und wofür der Benutzer diese Regel nutzen soll. Dieser Text wird dann im Assistenten angezeigt, wenn mehr als eine Gruppe konfiguriert und wählbar ist.

3. Auf dem Reiter **SB-Freigabe** wählen Sie die freizugebenden Gerätetypen und Module sowie die Zeit für die Freigabe aus.
   Wenn Sie **Vereinfachte Modulauswahl im Assistenten verwenden** auswählen, werden dem Benutzer nur genau diese Optionen und keine erweiterten Optionen angeboten. Aktivieren Sie die Option **Modulauswahl ausblenden, alle erlaubten Module freigeben**, dann kann bzw. muss der Benutzer keine Auswahl mehr treffen.

4. Auf dem Reiter **Optionen** geben Sie beispielsweise an, ob Endbenutzer Verwendungsrichtlinien akzeptieren müssen, bevor sie die Freigabe starten dürfen. Auch können Sie hier festlegen, dass die Freigabe beendet wird, sobald sich der Endbenutzer abmeldet.

5. Auf den Reitern **Angemeldete Benutzer** und **Computer** fügen Sie die Windows-Benutzer hinzu, die den Freigabe-Assistenten verwenden dürfen und die Computer, auf denen diese Benutzer mit dem Assistenten freigeben dürfen. Wenn Sie die Option

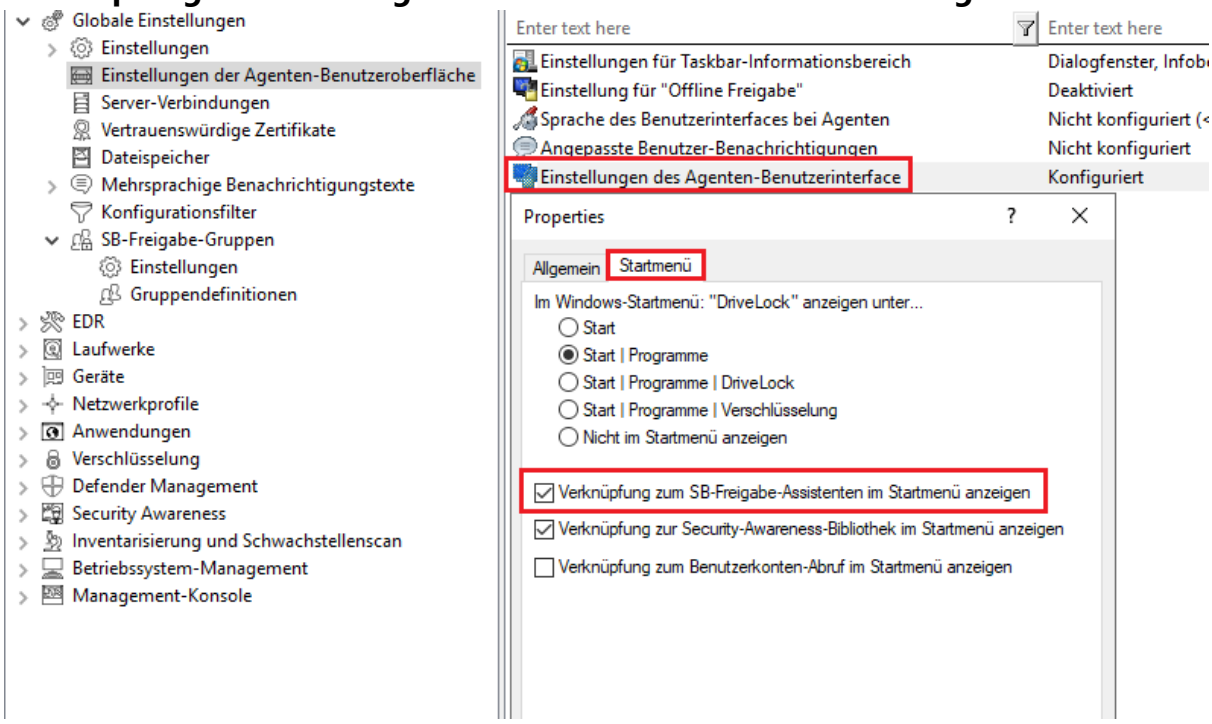
Nur < Lokaler Computer > freigeben wählen, kann ein Endbenutzer jeden Computer freigeben, für den diese Richtlinie gilt und auf dem er den Freigabe-Assistenten lokal starten kann. Sie können auch DriveLock Gruppen, Computernamen oder Active Directory Computer, Gruppen oder OUs hinzufügen.

Einen Anwendungsfall für die SB-Freigabe finden Sie hier.

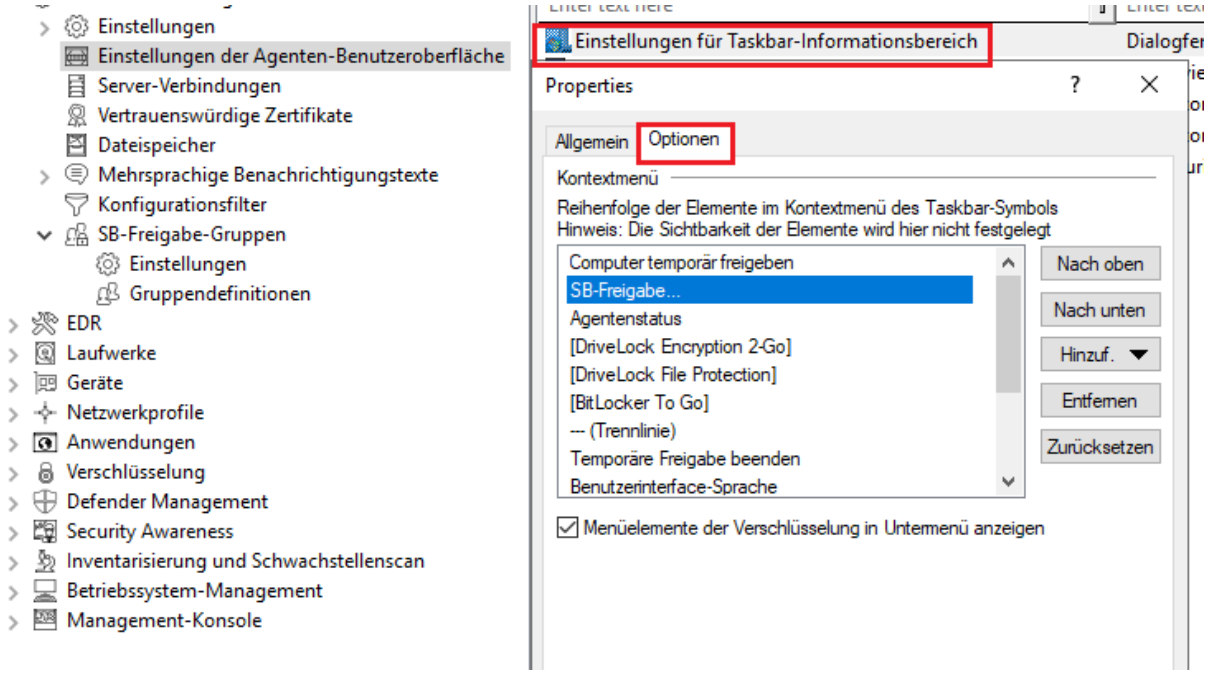
5.2.8.3 SB-Freigabe-Assistent aktivieren

Der SB-Freigabe-Assistent wird dem Endanwender standardmäßig nicht angeboten. Sie können diese Möglichkeit in einer Richtlinie an folgenden Stellen aktivieren:

1. In den **Einstellungen des Agenten-Benutzerinterface** auf dem Reiter **Startmenü**: **Verknüpfung zum SB-Freigabe-Assistenten im Startmenü anzeigen**.



2. In den **Einstellungen für Taskbar-Informationsbereich** auf dem Reiter Optionen. Fügen Sie die SB-Freigabe... hinzu und setzen Sie den Eintrag an die gewünschte Stelle.



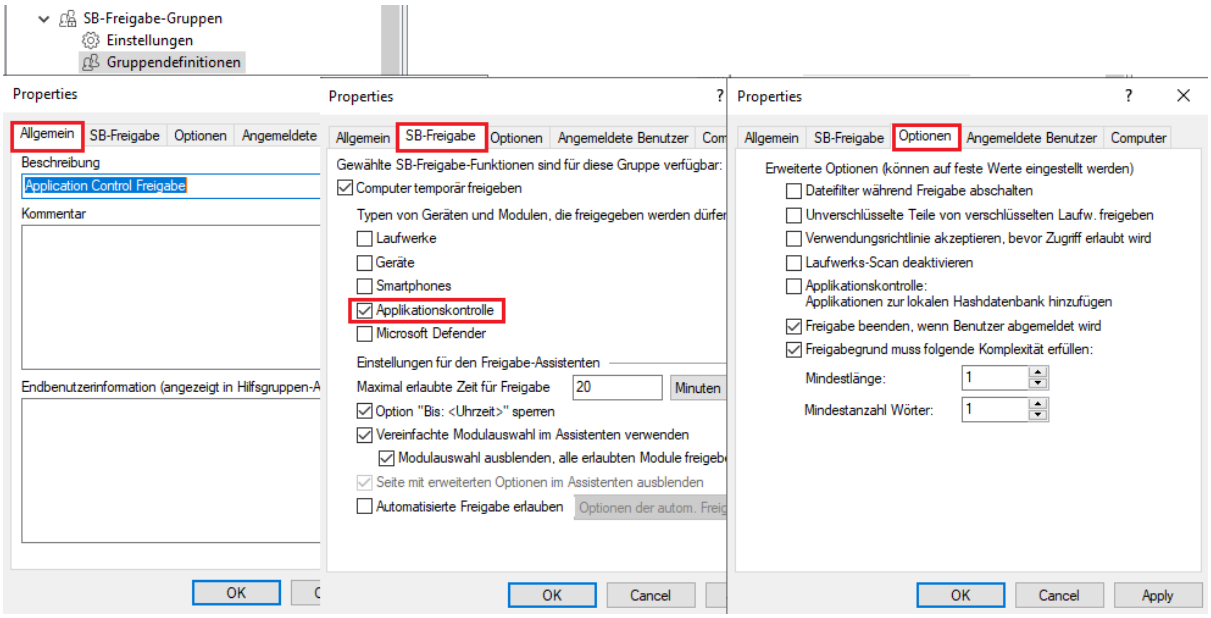
3. Sie können auch einrichten, dass der SB-Freigabe-Assistent gestartet wird, sobald eine Verwendungsrichtlinie angewendet wird. Mehr dazu finden Sie hier.

5.2.8.4 Anwendungsfall für SB-Freigabe: Application Control

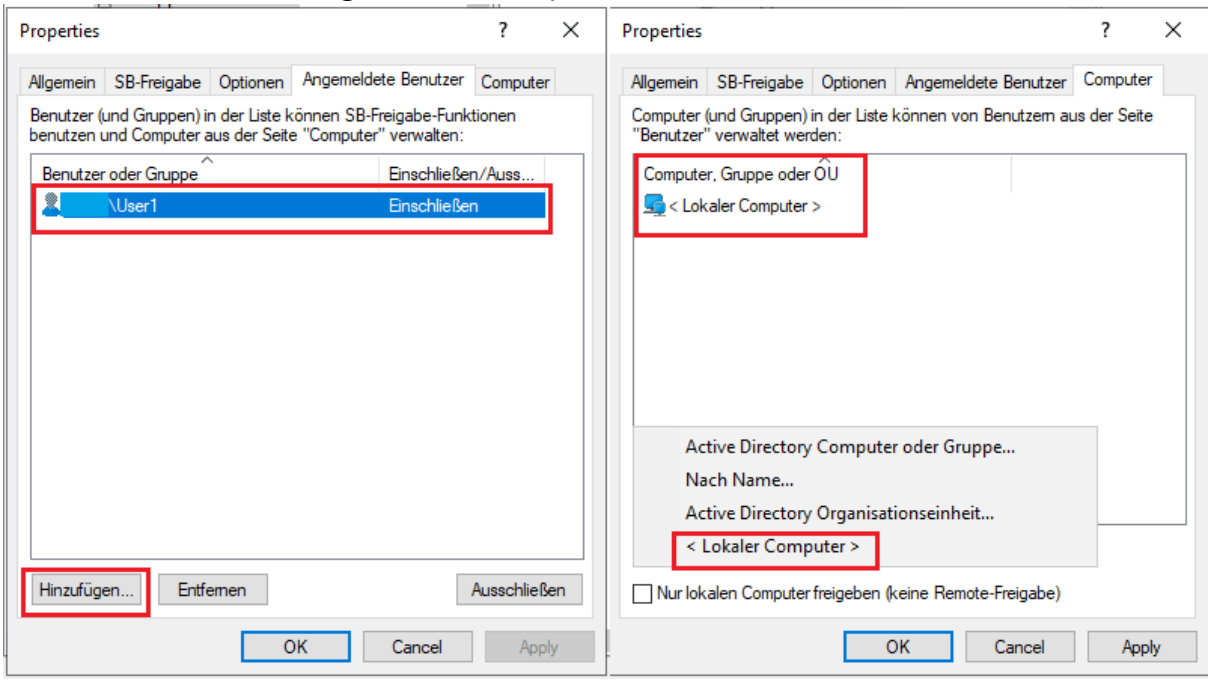
Ziel: Einfache SB-Freigabe mit dem Ziel, dass bestimmte Benutzer in Notfällen oder bei Wartungsarbeiten Anwendungen ausführen können, die nicht auf der Whitelist stehen. Hierbei wird mit Hilfe der SB-Freigabe Application Control zeitweise deaktiviert. Die lokale Whitelist wird dabei weder geändert, noch erweitert.

Gehen Sie folgendermaßen vor:

1. Erstellen Sie eine neue SB-Gruppe. Details finden Sie hier.
2. Vergeben Sie auf dem Reiter **Allgemein** eine Beschreibung und setzen Sie die Optionen auf den Reitern **SB-Freigabe** und **Optionen** wie in der Abbildung:



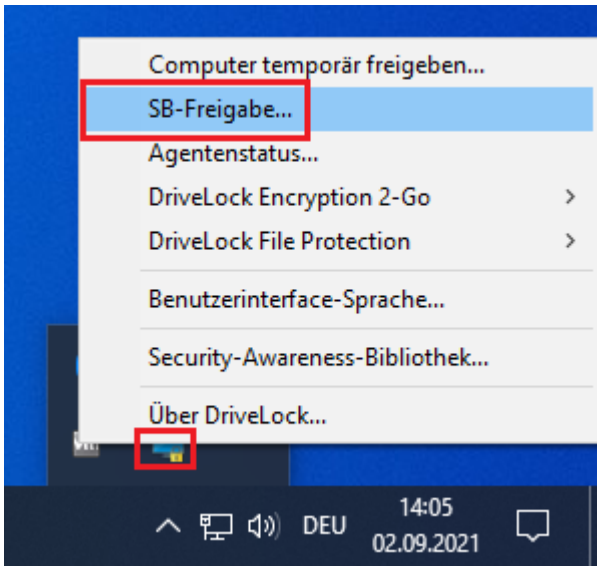
3. Wählen Sie auf den Reitern **Angemeldete Benutzer** und **Computer** die Benutzer und Computer aus, denen Sie die SB-Freigabe ermöglichen wollen. Verwenden Sie hierfür die Schaltfläche Hinzufügen. Siehe Beispiel unten:



4. Setzen Sie die entsprechenden Einstellungen für die SB Freigabe in den **Globalen Einstellungen**, wie hier (unter 1. und 2.) beschrieben.

5. Veröffentlichen Sie die Richtlinie und weisen Sie diese zu.

6. Auf dem DriveLock Agenten kann der Endbenutzer jetzt den SB-Freigabe-Assistent über das Symbol in der Taskleiste starten und dann in der eingestellten Zeit mit der benötigten Anwendung arbeiten.



5.3 Ereignisse und Alerts

Sie können alle Ereignisse, die im Zusammenhang mit DriveLock und dessen Modulen auftreten, überwachen und konfigurieren.

Die Basisfunktionalität beinhaltet neben der Übermittlung von DriveLock-Ereignissen auch die Möglichkeit, auf diese Ereignisse zu reagieren.

Risk & Compliance (EDR) bietet zudem weitere Funktionalitäten:

- Ereignisse von Drittanbietern überwachen,
- Filter, Alerts und Responses definieren und verwenden,
- Teile der Application Behavior Control-Funktionalität anwenden,
- Teile des MITRE Attack Frameworks verwenden, das in Form von importierbaren DriveLock-Regeln mitgeliefert wird.

Weiterführende Informationen zum Thema MITRE Attack und Application Control finden Sie in der gleichnamigen Dokumentation auf DriveLock Online Help.

5.3.1 Ereignisübermittlung

Bevor DriveLock Aktionen protokolliert werden können, muss erst eingestellt werden, dass DriveLock Ereignisse übertragen werden. Ereignisse können zur Windows Ereignisanzeige, SNMP, SMTP (Email) gesendet werden oder aber in die zentrale DriveLock Datenbank geschrieben werden.

Es gibt zwei Ereignisquellen, die gemeinsam konfiguriert werden:

- DriveLock Agenten Ereignisse (Quelle: “DriveLock”)
- DriveLock Management Konsolen Ereignisse (Quelle: “DriveLockMMC”)

Um DriveLock Ereignisse zu analysieren, empfehlen wir das DriveLock Operations Center.

Bei der Speicherung der DriveLock Ereignisse in der eigenen zentralen Datenbank können diese auf Wunsch auch anonymisiert werden, in dem sowohl der Benutzer- und der Computername ausschließlich verschlüsselt gespeichert werden. Eine Entschlüsselung ist dann z.B. nur nach dem 4-Augen-Prinzip möglich, wobei ebenso ein X-Augen-Prinzip konfiguriert werden kann wenn mehrere Personen zur Datenentschlüsselung notwendig sein sollen. Dadurch bleiben personenbezogene Daten geschützt.

5.3.1.1 Konfiguration der Ereignisübermittlung

Sie können die Protokollierung und den Speicherort der DriveLock-Ereignismeldungen konfigurieren. Wenn Sie ein entferntes Ziel konfigurieren und der Computer nicht mit dem Netzwerk verbunden ist, werden alle Meldungen vorübergehend auf dem lokalen Computer gespeichert.

Öffnen Sie in der DriveLock Management-Konsole in der Konsolenstruktur auf der linken Seite den Knoten **Ereignisse und Alerts** und dann den Unterknoten **DriveLock Ereignisse**. In diesem Unterknoten sind alle Ereignisse nach den Komponenten gruppiert, die sie erzeugen. Wenn Sie einen Knoten auswählen, wird im rechten Fensterbereich eine Liste der verfügbaren Ereignisse angezeigt.

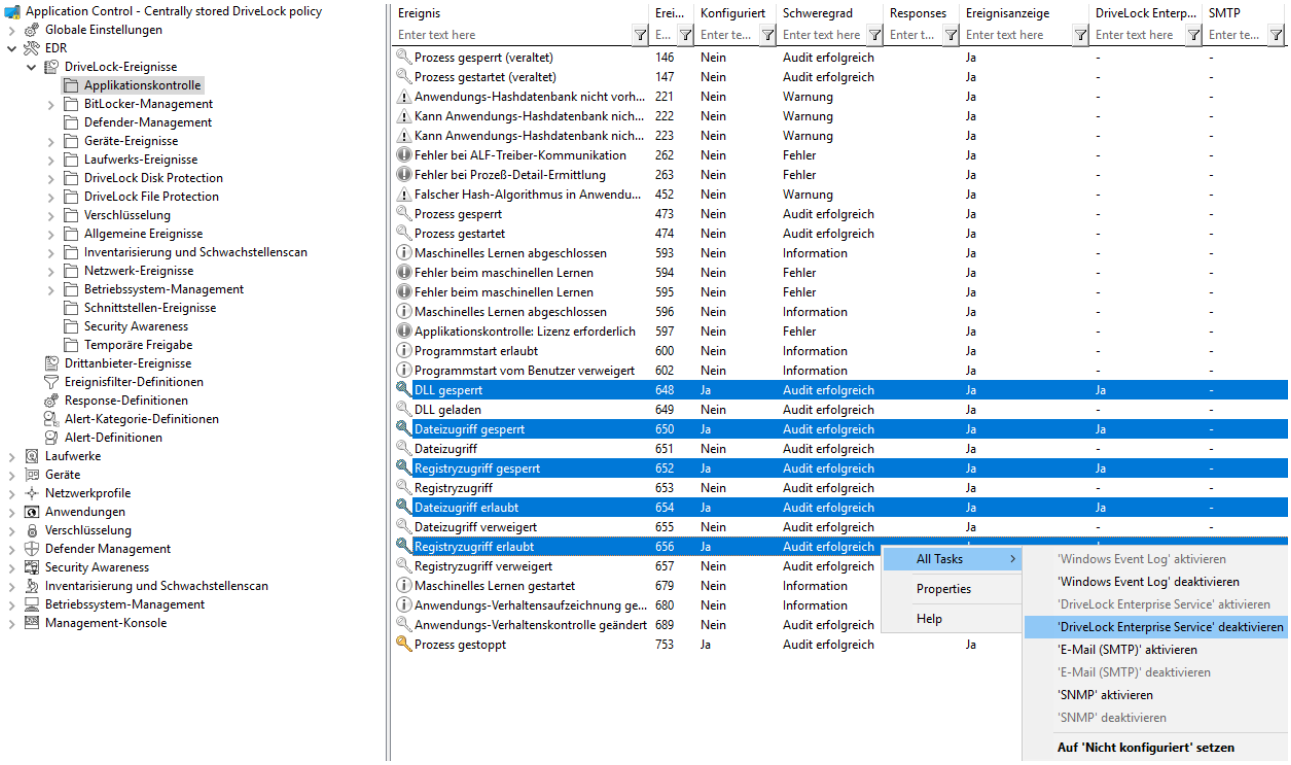
Um die Einstellungen für ein bestimmtes Ereignis zu ändern, doppelklicken Sie auf dieses Ereignis, um das zugehörige Eigenschaftsdialogfeld zu öffnen. Auf dem Reiter **Allgemein** können Sie festlegen, wohin dieses Ereignis gesendet werden soll (mehrere Ziele sind möglich) und ob mehrere Vorkommnisse in einem kurzen Zeitintervall unterdrückt werden sollen, um in der Protokolldatei bzw. den Protokolldateien weniger Speicherplatz zu beanspruchen.

Die angegebenen Ziele müssen weiter konfiguriert werden.

Auf dem Reiter **Responses** kann eine bestimmte Aktion ausgelöst werden, wenn dieses Ereignis eintritt. Die Aktion muss zuvor als Response-Definition beschrieben werden; Einzelheiten dazu finden Sie hier. Der Reiter **Ereignis-Info** zeigt den Ereignistext und die Parameter im Detail. Diese Informationen sind bei der Erstellung von Ereignisfiltern nützlich.

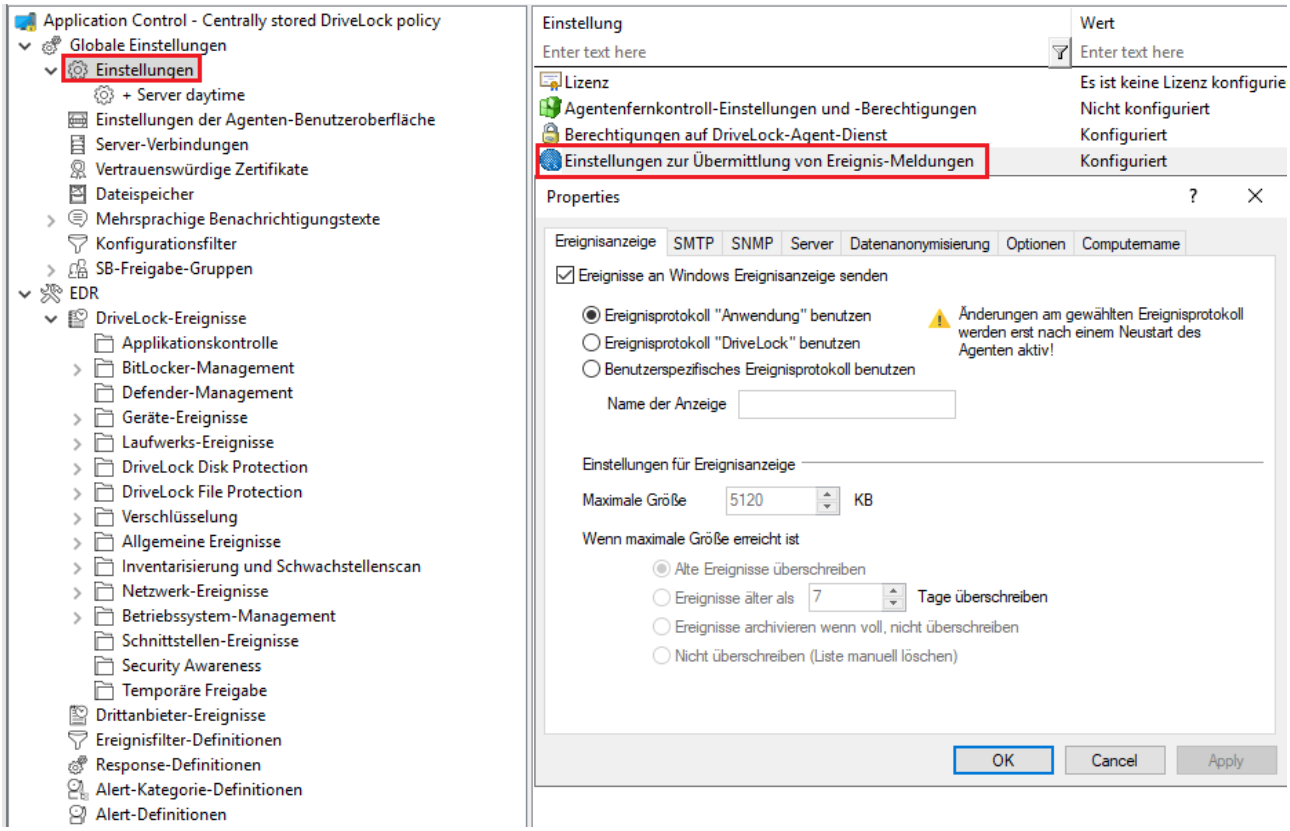
Um mehrere Ereignisse schnell an ein Ziel zu leiten, wählen Sie sie im rechten Fensterbereich aus (mit Umschalt- und Strg-Klick) und klicken Sie dann mit der rechten Maustaste auf die Auswahl. Das sich öffnende Kontextmenü enthält ein Untermenü **Alle**

Aufgaben / All Tasks, das Optionen zum Aktivieren oder Deaktivieren jedes verfügbaren Ereignisziels für alle ausgewählten Ereignisse enthält.



5.3.1.2 Ziele der Ereignisübermittlung

Jedes der möglichen Ziele, an die Ereignisse gesendet werden können, erfordert unterschiedliche spezifische Einstellungen. Um Ziele für die Übermittlung von Ereignissen zu konfigurieren, öffnen Sie den Knoten **Globale Einstellungen** in der Konsolenstruktur auf der linken Seite und wählen Sie **Einstellungen**. Klicken Sie dann im rechten Fensterbereich auf **Einstellungen zur Übermittlung von Ereignis-Meldungen**, um das Einstellungsdialogfeld zu öffnen. Die einzelnen Reiter dieses Dialogfelds werden im Folgenden beschrieben.



5.3.1.2.1 Ereignisanzeige

Auf dem Reiter **Ereignisanzeige** konfigurieren Sie, welches Ereignisprotokoll DriveLock verwendet, um die Ereignisse lokal zu speichern. Diese Einstellung legt fest, ob die Ereignisse des Agenten in die Windows Anwendungs-Ereignisanzeige oder in ein anderes Ereignisprotokoll geschrieben werden. Wenn Sie nicht die Windows Anwendungs-Ereignisanzeige benutzen, legen Sie die Größe und das Verhalten fest, wenn der Protokollspeicher voll wird.

5.3.1.2.2 SMTP

Wählen Sie den Reiter **SMTP**, um SMTP-Einstellungen für den Versand von Ereignisnachrichten per E-Mail zu konfigurieren.

Wählen Sie **SMTP-Nachrichtenübertragung aktivieren**, um die Ereignisprotokoll-Nachrichtenübertragung zu aktivieren. Geben Sie die benötigten Server-Eigenschaften ein und stellen Sie sicher, dass Nachrichten von Ihrem E-Mail System akzeptiert werden. Wenn Ihr Mail-Server eine Authentifizierung erfordert, müssen Sie auch Authentifizierungsdaten angeben.

Klicken Sie auf die Schaltfläche **Nachrichtentext**, um die eigentliche E-Mail zu konfigurieren. Über die beiden > Schaltflächen rechts können vordefinierte Platzhalter in den

Text eingefügt werden, die zum Ausführungszeitpunkt mit aktuellen Werten gefüllt werden. Eine E-Mail kann sowohl als Text als auch als HTML-E-Mail versendet werden.

Klicken Sie auf **Test**, um eine Test Email zu den konfigurierten Empfängern zu senden. Sie erhalten anschließend eine entsprechende Nachricht angezeigt, die Ihnen Auskunft darüber gibt, ob alle Parameter richtig konfiguriert wurden.

5.3.1.2.3 SNMP

Auf dem Reiter **SNMP** aktivieren Sie Option Nachrichtenübertragung über SNMP Traps aktivieren, um die Ereignisse über SNMP zu übertragen und geben Sie die benötigten Server-Eigenschaften an.

5.3.1.2.4 Server

Klicken Sie auf den Reiter **Server**, um die Übertragungs-Einstellungen für den DriveLock Enterprise Service zu konfigurieren.

Wählen Sie **Ereignisse an DriveLock Enterprise Service senden** aus, um die Ereignisübertragung zur zentralen DriveLock Datenbank zu aktivieren.

Wählen Sie **Agenten-Status zu Server senden**, wenn Sie das Zeitintervall der Übertragung angeben möchten. Der DriveLock Agent wird standardmäßig alle 300 Sekunden seine Ereignisse zum DriveLock Enterprise Service senden.

> Hinweis: Beachten Sie, dass die Server-Verbindung unter Globale Einstellungen / Server-Verbindungen konfiguriert werden muss.

5.3.1.2.5 Datenanonymisierung

In manchen Bereichen müssen gesetzliche Bestimmungen im Umgang mit personenbezogenen Daten und deren automatisierter Erfassung beachtet werden. Das gilt insbesondere dann, wenn die zentrale Speicherung derartiger Daten von anderen Personen zu Auswertungen verwendet werden könnte. Um sich daraus ergebenden Anforderungen auf einfachste Weise gerecht zu werden, haben Sie in DriveLock an dieser Stelle die Möglichkeit einzustellen, dass Ereignisdaten vor der Übermittlung an andere Systeme (wie z.B. die zentrale DriveLock Datenbank) anonymisiert werden. Die Konfigurationsoptionen dazu finden Sie auf dem Reiter **Datenanonymisierung**.

Standardmäßig werden sowohl der Computername als auch der Name des aktuellen Benutzers im Klartext übertragen bzw. gespeichert. An dieser Stelle können Sie nun zwei weitere Optionen getrennt für Benutzername und Computername konfigurieren:

- **Inhalt verschlüsseln**: Benutzername und/oder Computername werden mit einem oder mehreren öffentlichen Schlüsseln verschlüsselt und dann übertragen. Bei Bedarf kann diese Information wieder entschlüsselt werden. Somit ist die Nachvollziehbarkeit bei einem bestimmten Ereignis mit Bezug auf einen Benutzer bzw. Computer wieder möglich.
- **Inhalt nicht speichern**: Benutzername und/oder Computername werden nicht übertragen. Somit ist die Nachvollziehbarkeit bei einem bestimmten Ereignis mit Bezug auf einen Benutzer bzw. Computer nachträglich nicht mehr möglich.

Hinweis: Eine Entschlüsselung von Benutzer- bzw. Computername ist nur bei Ereignissen möglich, die an die zentrale DriveLock Datenbank übertragen und dort gespeichert wurden. Bei Ereignisse, die per SMTP oder SNMP übertragen wurden, können verschlüsselte Felder nicht wieder de-anonymisiert (d.h. entschlüsselt) werden.

Haben Sie bei einem der beiden Felder (**Computer- oder Benutzerinformation**) die Verschlüsselung aktiviert, müssen Sie zusätzlich mindestens noch ein Zertifikat angeben, welches die zur Ver- bzw. Entschlüsselung verwendeten Schlüssel enthält.

Klicken Sie dazu auf **Hinzufügen** und wählen Sie aus, ob Sie ein bereits bestehendes Zertifikat verwenden möchten (welches als Datei vorliegt), oder ob ein neues Zertifikat generiert werden soll. Klicken Sie für Letzteres auf **Neu anlegen**. Dadurch wird der Assistent für die Erzeugung des Verschlüsselungszertifikates gestartet.

Geben Sie entweder den Ordner an, wo Sie die Zertifikats-Datei abspeichern möchten oder wählen Sie alternativ eine Smartcard als Speicherort. Zertifikatsdateien werden immer unter den gleichen Dateinamen gespeichert:

- DLEventEncrypt.cer für die Zertifikatsdatei,
- DLEventEncrypt.pfx für die PKCS#12-Datei, die sowohl das Zertifikat als auch den passenden privaten Schlüssel enthält.

Wenn Sie zwei Zertifikate im gleichen Ordner speichern möchten, müssen Sie diese Dateien vor der Erstellung des zweiten Zertifikats umbenennen. Wenn Sie versuchen, ein Zertifikat im gleichen Ordner zu speichern, in dem bereits ein anderes gleichnamiges Zertifikat vor-

handen ist, warnt Sie der Assistent und fordert Sie auf, einen anderen Speicherort für die Zertifikatsdateien zu wählen.

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

Hinweis: Die verwendete Smartcard (bzw. auch ein entsprechendes Token zum Speichern von Zertifikaten) muss aus technischen Gründen zwingend in der Lage sein, den privaten Schlüssel des Zertifikates exportieren zu können. Ansonsten ist eine Entschlüsselung später damit nicht möglich. Sofern Sie sich nicht sicher sind, ob die verwendete Smartcard oder das Token dies unterstützt, führen Sie zunächst einen entsprechenden Test durch.

Achtung: Speichern Sie die Zertifikatsdateien (.pfx) oder Smartcards an einem sicheren Ort, um zu gewährleisten, dass sie verfügbar sind, wenn Sie künftig Ereignisdaten entschlüsseln müssen. Wenn eines der Zertifikate verloren geht, ist eine Entschlüsselung nicht mehr möglich!

Geben Sie nun das Passwort für den Zugriff auf den privaten Schlüsselbereich des Zertifikates an, z.B. Zugriff auf die Datei DLEventEncrypt.pfx. Stellen Sie sicher, dieses Passwort nicht zu vergessen und bewahren Sie es sicher auf.

Es dauert einige Sekunden, um das Zertifikat zu erzeugen. Anschließend werden Sie benachrichtigt, wenn der Prozess abgeschlossen ist und die Datei an dem zuvor angegebenen Ort abgespeichert wurde. Sofern eine Smartcard zur Speicherung verwendet wird, werden Sie aufgefordert, die PIN für den Zugriff auf die Smartcard einzugeben.

Nachdem das Zertifikat erzeugt wurde, erscheint es in der Liste der Zertifikate. Sie können nun weitere Zertifikate generieren, die alle für die Ver- aber auch Entschlüsselung benötigt werden. Sie könnten z.B. je einen Vertreter Ihrer Rechtsabteilung und Ihrer Personalabteilung mit der Entschlüsselung beauftragen. Dazu müssten Sie zwei Sätze von Zertifikatsdateien konfigurieren und dem Vertreter jeder Abteilung einen davon aushändigen.

Wenn Sie ein Zertifikat auswählen und auf **Eigenschaften** klicken, erhalten Sie zusätzliche Informationen über das Zertifikat.

Das Zertifikat wird ebenfalls in dem privaten Zertifikatsspeichers des aktuellen Benutzers gespeichert.

Achtung: Da alle generierten Zertifikate beim Generieren auch im Zertifikatsspeicher des aktuellen Benutzers abgelegt werden, müssen Sie ggf. zur

Umsetzung eines strikten Mehr-Augen-Prinzips eines oder mehrere Zertifikate wieder daraus löschen, da ansonsten dieser Benutzer die Entschlüsselung alleine vornehmen könnte (sofern er auch die Passwörter für den Zugriff darauf hat).

Sobald Sie die Einstellungen übernehmen und der DriveLock Agent diese neue Richtlinie erhält, werden die ausgewählten Felder ab sofort verschlüsselt.

5.3.1.2.6 Optionen

Auf dem Reiter **Optionen** können Sie festlegen, wie DriveLock Nachrichten des DriveLock Enterprise Service verarbeitet, wenn der Client offline ist. Ereignisnachrichten können lokal zwischengespeichert werden, wenn der DriveLock Agent sie nicht an das konfigurierte Ziel übermitteln kann.

Wählen Sie **Ereignisse sammeln, wenn Computer offline**, um die temporäre Speicherung von Nachrichten zu aktivieren. DriveLock Agenten verwenden immer eine interne speicherbasierte Warteschlange, um Ereignisse vorübergehend zu speichern, wenn sie schneller erzeugt werden, als sie verarbeitet werden können. Darüber hinaus können Sie den Agenten so konfigurieren, dass er Ereignisse in einer festplattenbasierten Warteschlange speichert, wenn der Agent offline ist und den DriveLock Enterprise Service nicht kontaktieren kann. Ereignisse werden automatisch aus beiden Warteschlangen gelöscht, sobald sie verarbeitet wurden. Sie können die maximale Anzahl von Nachrichten konfigurieren, die diese Warteschlangen aufnehmen können. Überschreitet eine der beiden Warteschlangen das von Ihnen konfigurierte Limit, werden zusätzliche Ereignisse nicht mehr an den DriveLock Enterprise Service weitergeleitet und nur noch in das lokale Ereignisprotokoll geschrieben.

In der Regel überträgt jeder Agent Ereignisdaten in Echtzeit an die von Ihnen konfigurierten Zielorte. In Systemumgebungen, in denen die verfügbare Netzwerkbandbreite begrenzt ist, kann der DriveLock Agent Ereignisse sammeln und mehrere Ereignisse zusammen in Paketen senden. Um diese Einstellung zu aktivieren, markieren Sie das Kontrollkästchen **Ereignisse in Paketen versenden** und konfigurieren Sie eine für Ihre Netzwerkumgebung geeignete Paketgröße und Intervall.

5.3.1.2.7 Computername

Wenn Sie nicht wollen, dass der Standard-Windows-Computername als Quelle für ein Ereignis gemeldet wird, bietet die Registerkarte **Computername** mehrere Optionen zum Anpassen des verwendeten Namens. Der Computername kann aus einem Registrierungsschlüssel, einer INI-Datei oder sogar von einer benutzerdefinierten DLL, die den Namen zurückgibt,

abgerufen werden. Wählen Sie das entsprechende Optionsfeld und geben Sie die für die gewählte Option erforderlichen Informationen ein.

5.3.1.3 Reaktion auf Ereignisse (Response)

Der DriveLock Agent kann nicht nur einfach Ereignismeldungen an verschiedene Ziele senden, sondern auch eine lokale Reaktion auf das Ereignis ('Response') initiieren, wenn das Ereignis eintritt. Eine solche Reaktion kann die Ausführung eines Programms oder Skripts sein oder die Aufnahme eines Fotos mit einer an das System angeschlossenen Webcam. Responses können bei einzelnen Ereignissen (siehe hier) und Alerts (siehe hier) verwendet werden, sobald diese definiert und benannt wurden.

Um eine neue **Response-Definition** zu erstellen, klicken Sie mit der rechten Maustaste auf Response-Definitionen, und wählen dann **Neu...** aus dem Kontextmenü. Die folgenden Response-Typen sind verfügbar:

- **PowerShell-Skript**: Führt ein genanntes PowerShell-Skript mit optionalen Parametern aus dem Ereignis aus, auf das sich die Response bezieht.
- **Batch-Skript**: Führt ein Batch-Skript mit dem Befehlsprozessor aus, optional mit Parametern.
- **Befehlszeilenausführung**: Startet eine beliebige ausführbare Datei, optional mit Parametern.
- **Anzeige einer Security-Awareness-Kampagne**: Zeigt eine definierte Awareness-Kampagne an, wenn das Ereignis eintritt.
- **Aufnahme mit Webcam**: Erstellt beim Eintreten des Ereignisses eine Aufnahme und überträgt sie zusammen mit dem Ereignis. Diese Option sollte mit Bedacht verwendet werden, da sie schnell viel Speicherplatz verbrauchen kann, wenn das Ereignis zu häufig ausgelöst wird.

Responses werden über ein Dialogfeld mit folgenden Reitern definiert.

Auf dem Reiter **Allgemein** können ein Name und ein optionaler Kommentar eingegeben werden.

Mithilfe der Reiter **Skript** oder **Kommandozeile** wird der auszuführende Befehl oder das Skript einschließlich aller Parameter erstellt. Die Befehlszeile kann einfach in das Textfeld eingegeben oder durch Auswahl einer ausführbaren Datei/Skript und aller erforderlichen Parameter erstellt werden. Zur Verwendung der Schaltfläche **Parameter einfügen** müssen die Parameter allerdings zuerst auf der Registerkarte Parameter definiert werden.

Bei allen Response-Typen stehen Ihnen verschiedene Optionen zur Verfügung, mit denen Sie Bedingungen für die Verwendung definieren können: Die Registerkarten **Computer**, **Netzwerke** und **Zeiten** können verwendet werden, um die Response zu aktivieren oder zu deaktivieren, wenn bestimmte Bedingungen erfüllt sind. Dadurch könnte z.B. die Response nur auf bestimmten Computern ausgelöst werden, während diese mit dem Firmennetzwerk verbunden sind und das Ereignis außerhalb der regulären Bürozeiten stattfindet.

Klicken Sie **OK**, sobald alle Einstellungen abgeschlossen sind, um die Response-Definition zu speichern. Sie wird der Liste der Response-Definitionen auf der rechten Seite hinzugefügt. Anhand dieser Liste kann dann eine Auswahl von Responses auf Ereignisse und Alerts getroffen werden.

5.3.1.4 Ereignisfilter-Definitionen

Mit Hilfe von Ereignisfiltern lassen sich bestimmte Instanzen eines Ereignisses auf der Grundlage der Ereignisparameter auswählen. Häufig enthalten Ereignisse neben der Ereignisnummer und der Nachricht zusätzliche Informationen. Diese Informationen können verwendet werden, um relevante von weniger relevanten Ereignissen zu unterscheiden. Durch die separate Definition von Ereignisfiltern können sie schnell in Regeln wiederverwendet werden, die eine Auswahl von Ereignissen erfordern.

Um einen Ereignisfilter zu erstellen, klicken Sie mit der rechten Maustaste auf den Unterknoten **Ereignisfilter-Definitionen** und wählen Sie **Neu...** aus dem Menü. Eine Liste der verfügbaren Ereignisse wird angezeigt. Wählen Sie das Ereignis aus, auf das dieser Filter angewendet werden soll, und klicken Sie **OK**.

Ein Dialogfeld mit Reitern wird angezeigt. Auf dem Reiter **Allgemein** kann im Feld **Beschreibung** ein Name für den Filter eingegeben werden - dies ist der Name, der in der Ereignisfilterliste angezeigt wird, sobald die Definition gespeichert ist.

Auf dem Reiter **Filterkriterien** wird festgelegt, wie die verschiedenen Instanzen des Ereignisses gefiltert werden sollen. Mit der Schaltfläche **Hinzufügen** können Kriterien und logische Operatoren zur Filterspezifikation hinzugefügt werden. Die verfügbaren Kriterien variieren je nach Ereignistyp, abhängig von den zusätzlichen Informationen, die mit dem Ereignis protokolliert werden. Die logischen Operatoren können verwendet werden, um mehrere Bedingungen für die Ereignisauswahl zu kombinieren.

Zur Beschreibung einer Bedingung beginnen Sie mit dem Hinzufügen eines Operators. Die folgenden Operatoren sind verfügbar:

- **UND**: Alle mit diesem Operator verbundenen Kriterien müssen übereinstimmen
- **ODER**: Mindestens eines der mit diesem Operator verbundenen Kriterien muß übereinstimmen
- **N**: Mindestens n Kriterien der aufgeführten (mehr als n) mit diesem Operator verbundenen Kriterien müssen übereinstimmen. Die Zahl n wird beim Hinzufügen des Operators ausgewählt.

Um ein Kriterium mit einem Operator zu verknüpfen, wählen Sie den Operator in der Liste aus, klicken Sie auf Hinzufügen und wählen Sie Kriterium. Wählen Sie aus der angezeigten Liste der Ereignisparameter einen aus. Im nächsten Dialogfeld wird das Kriterium vervollständigt, indem ein Vergleichs- oder Übereinstimmungsoperator und ein oder mehrere Wert(e) zum Vergleich ausgewählt werden. Um das Kriterium zur Filterbeschreibung hinzuzufügen, klicken Sie auf OK.

Sie können Operatoren und Bedingungen ändern, indem Sie sie auswählen und auf die Schaltfläche **Bearbeiten** klicken.

Die Registerkarten **Computer**, **Netzwerke** und **Zeiten** können verwendet werden, um die Verwendung des Filters auf bestimmten Computern, die an bestimmte Netzwerke angeschlossen sind, während bestimmter Zeiträume zu aktivieren oder zu deaktivieren.

Speichern Sie die neue Filterdefinition. Sie wird der Liste der Ereignisfilterdefinitionen auf der rechten Seite hinzugefügt.

5.3.1.5 Alerts

Bei Alerts handelt es sich um ein Mittel zur Erzeugung eines Meta-Ereignisses, wenn z.B. bestimmte Kombinationen von Ereignissen innerhalb eines kurzen Zeitintervalls auftreten. Anstatt nach Mustern in Ereignisprotokollen zu suchen, kann eine Alert-Definition verwendet werden, um ein solches Muster zu erkennen und sofort zu melden. Ein Alert kann nicht nur die Erkennung melden, sondern auch eine entsprechende Response auslösen.

> Hinweis: Bitte beachten Sie, dass bei konfigurierter Ereignisverschlüsselung der Inhalt der Ereignisse im Alert unverschlüsselt im DriveLock Operations Center (DOC) und in der eventuell definierten Response dargestellt wird, um geschäftskritische Ereignisse (zB. Datendiebstahl) verzögerungsfrei und mit brauchbarem Inhalt melden zu können.

Um eine Alert-Definition zu erstellen, klicken Sie mit der rechten Maustaste auf den Unterknoten **Alert-Definitionen** und wählen Sie **Neu...** aus dem Menü. Ein Dialog mit mehreren Reitern wird angezeigt.

Auf dem Reiter **Allgemein** kann im Feld **Beschreibung** ein Name für den Alert eingegeben werden - dies ist der Name, der in der Liste der Alert-Definitionen angezeigt wird, sobald die Definition gespeichert wurde. Darüber hinaus können eine **Schweregrad-** und eine **Alert-Kategorie** eingestellt werden, um die Alert-Berichte im DOC besser zu organisieren. Alert-Kategorien müssen in den Unterknoten Alert-Kategorie-Definitionen des Ereignisse und Alerts-Knotens definiert werden und werden auf dem Server verwaltet.

Auf dem Reiter **Bedingungen** werden die Kriterien für die Auslösung des Alerts definiert. Verwenden Sie die Schaltfläche **Hinzufügen**, um logische Operatoren und Kriterien hinzuzufügen, die die Bedingung(en) für den Alert beschreiben.

Die einfachste Bedingung, die für einen Alert verwendet werden kann, ist die Übereinstimmung mit einem einzelnen Ereignisfilter. Klicken Sie dazu einfach auf **Hinzufügen, Kriterium**, und wählen Sie den passenden Ereignisfilter aus der Liste aus.

Es ist auch möglich, mehrere Ereignisfilter zu kombinieren: Zuerst fügen Sie einen der logischen Operatoren **AND**, **OR** oder **N** hinzu. Wählen Sie dann den Operator in der Bedingungsliste aus und klicken Sie erneut auf **Hinzufügen**, um mit dem Hinzufügen von Kriterien zu beginnen, auf die der Operator angewendet werden soll. Die Auswahl des Kriteriums öffnet die **Liste der Ereignisfilter** zur Auswahl eines Filters, der in die Bedingung einbezogen werden soll. Fahren Sie mit dem Hinzufügen eines Kriteriums fort, bis alle erforderlichen Ereignisfilter unter dem ausgewählten Operator aufgelistet sind. Achten Sie darauf, im Feld **Ereignisse für diese Bedingung müssen innerhalb von ... Sekunden auftreten** ein geeignetes Zeitfenster zu wählen, um zu verhindern, dass die Bedingung auf Ereignisse trifft, die in keinem Zusammenhang stehen und falsche Alerts auslösen.

Auf dem Reiter **Responses** kann zusätzlich zur Meldung des Alerts eine Sofortreaktion eingerichtet werden. Wählen Sie in der Dropdown-Liste **Auszuführende Response** eine Response aus der Liste der Response-Definitionen aus. Die Parameterdefinitionen für diese Antwort werden in der Liste **Parameter-Mapping** angezeigt. Wählen Sie einen Parameter und klicken Sie auf die Schaltfläche Bearbeiten, um den Parameterwert anzupassen, der in diesem Alert verwendet werden soll, wenn der Wert in der Response-Definition nicht geeignet ist.

Die Registerkarten **Computer**, **Netzwerke** und **Zeiten** können verwendet werden, um die Verwendung des Filters auf bestimmten Computern, die an bestimmte Netzwerke angeschlossen sind, während bestimmter Zeiträume zu aktivieren oder zu deaktivieren.

Speichern die neue Filterdefinition. Sie wird der Liste der Alert-Definitionen auf der rechten Seite hinzugefügt.

5.3.2 Datenmaskierung in Ereignissen

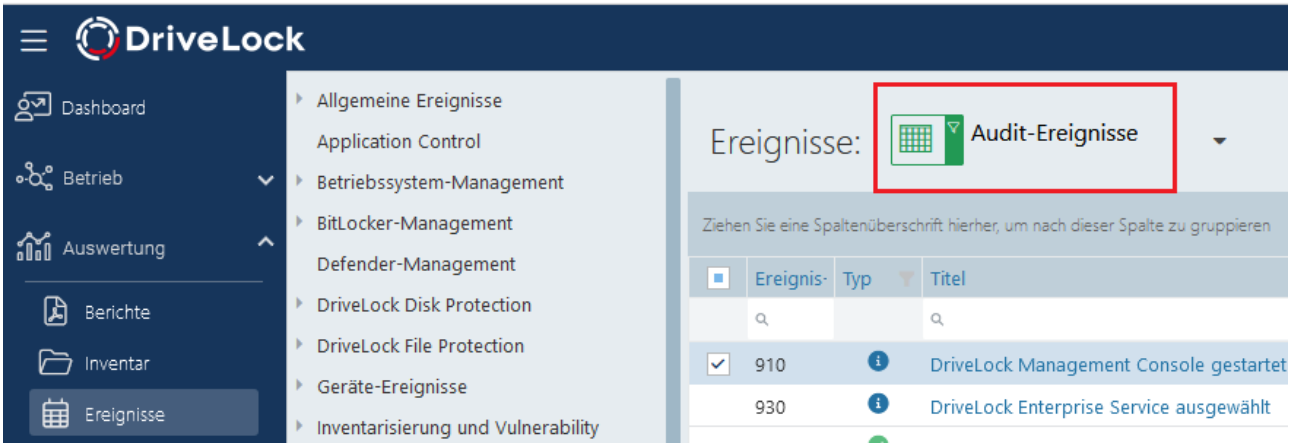
Bitte beachten Sie, dass im DOC die Namen bei aktiver Datenmaskierung und Filterung auf Benutzer- und Computernamen nicht in Klartext angezeigt werden. Systembenutzernamen werden standardmäßig immer angezeigt, durch Deaktivieren der Option **'Integrierter Benutzer' in Klartext anzeigen** können diese aber auch maskiert werden. Sie können auf diese filtern, indem Sie die Filtereigenschaft **Ist Systembenutzer** verwenden.

5.3.3 Audit-Ereignisse

Audit-Ereignisse sind Ereignisse zur Nachverfolgung von administrativen und sicherheitsrelevanten Aktionen, die von den DriveLock-Konten im DOC und in der MMC ausgelöst werden, z. B. beim Ändern von Richtlinien oder Berechtigungen.

Audit-Ereignisse können wie andere Ereignisse bearbeitet werden. In der Datenbank werden sie mit einem Flag markiert.

Um sich Audit-Ereignisse anzeigen zu lassen, können Sie im DOC in der Ansicht **Ereignisse** den Filter **Audit-Ereignisse** wählen (s. Abbildung).



Eine Liste aller Ereignisse und Audit-Ereignisse finden Sie in der DriveLock Events Dokumentation auf DriveLock Online Help.

5.4 Laufwerke und Geräte / Device Control

Mit DriveLock Device Control können sämtliche Wechseldatenträger und externe Geräte und Laufwerke kontrolliert werden. Mithilfe von Regeln (Whitelist oder Blacklist) wird die Zulässigkeit von Aktionen definiert.

Device Control bietet u.a. folgende Funktionalitäten:

- Kontrolle aller extern angeschlossenen Medien: Sie legen fest, wer zu welchem Zeitpunkt welche Laufwerke verwenden darf.
- Integrierte Datenflusskontrolle durch Datentyp-Prüfung: Sie legen fest, wer welche Daten lesen oder kopieren darf.
- Audit von Dateioperationen: Sie kontrollieren, wer zu welchem Zeitpunkt welche Datei auf welches Medium kopiert hat.
- Sicherheit bei Netzwerkfreigaben oder WebDAV-basierten Laufwerken: Sie legen fest, wer zu welchem Zeitpunkt welche Laufwerke verwenden darf.
- Erstellung von Schattenkopien und erzwungene Verschlüsselung
- Kontrolle des Datenvolumens: Sie legen fest, wie hoch das Datenvolumen sein darf, das zwischen Wechseldatenträger und Endgerät transferiert wird,

5.4.1 Geräte

DriveLock arbeitet mit Whitelist-Regeln. Dieses Grundprinzip bedeutet, dass nach Aktivierung der Sperrung alle Geräte zunächst gesperrt sind und nur für die zugelassenen Geräte (bzw. Gerätegruppen oder Gerätelisten) eigene Whitelist-Regeln erstellt werden müssen, mit denen die Verwendung erlaubt wird.

Dabei können Regeln für unterschiedliche Geltungsbereiche auf unterschiedlichen Ebenen zusammengefasst werden:

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

Außerdem können Sie definieren, auf welchen Computern, für welche Netzwerkverbindungen, für welche Benutzer und zu welcher Zeit Whitelist-Regeln angewendet werden.

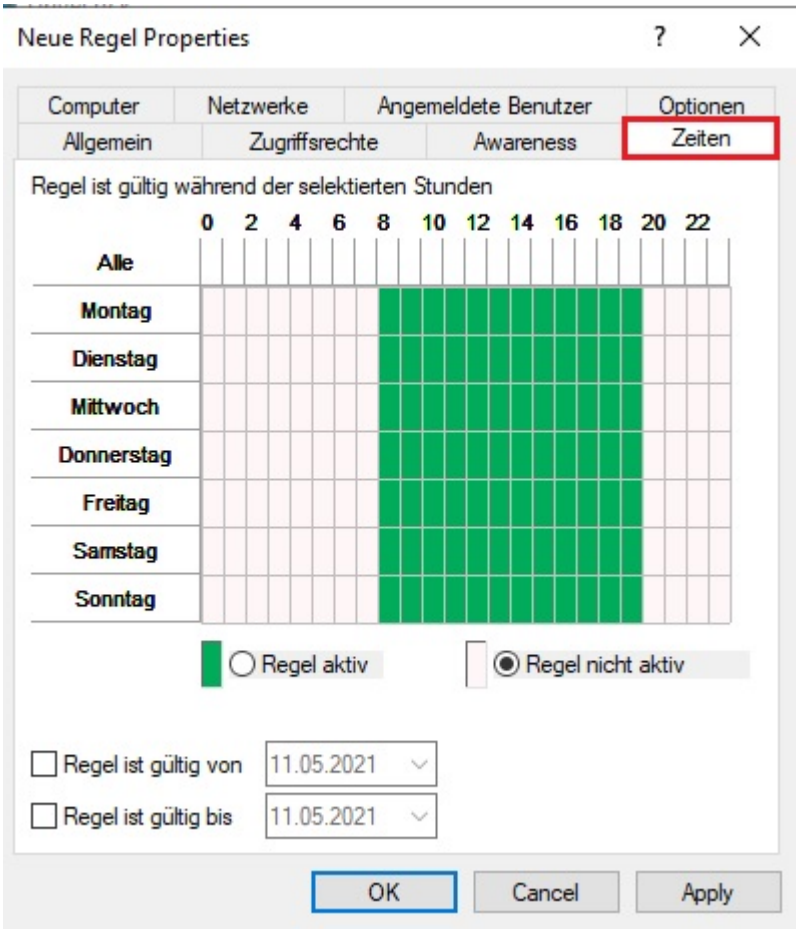
5.4.2 Modulübergreifende Einstellungen in Regeln

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

5.4.2.1 Zeitliche Einschränkungen

Damit eine Regel nur für einen ganz bestimmten Zeitraum gilt, können Sie einen individuellen Zeitrahmen auf dem Reiter **Zeiten** vorgeben (z.B. nur werktags von 08:00 Uhr bis

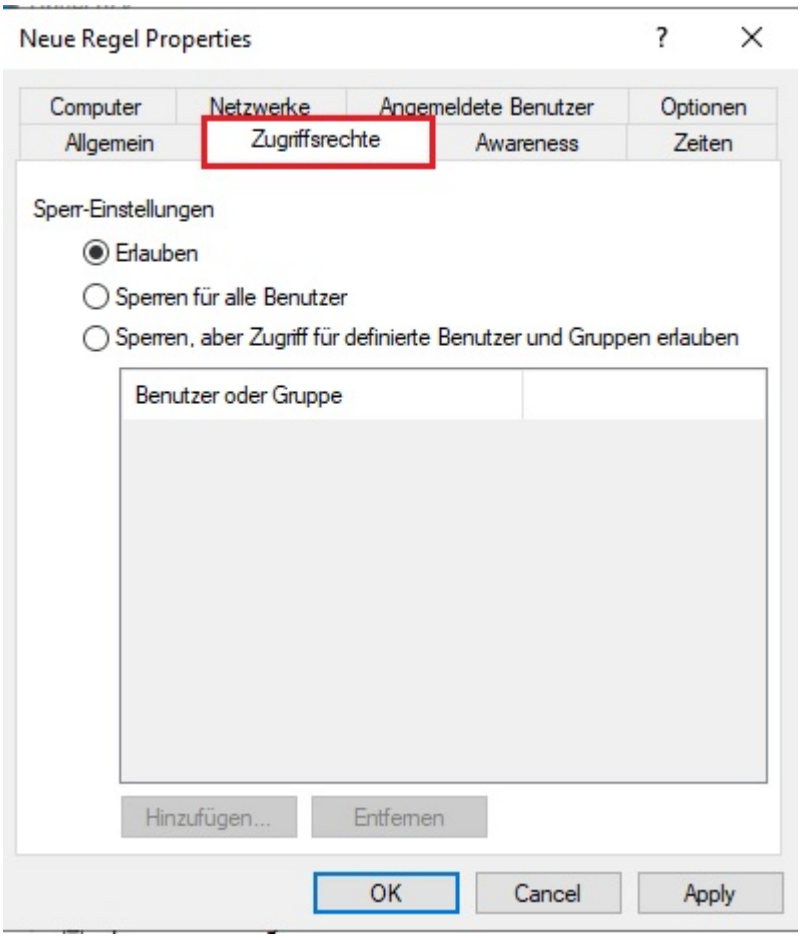
19:00 Uhr). Es ist ebenso möglich, ein Datum für den Beginn und das Ende der Gültigkeitsdauer anzugeben.



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

5.4.2.2 Zugriffsberechtigungen für Benutzer und Gruppen

Wählen Sie den Reiter Zugriffsrechte, um festzulegen, welche Benutzer bzw. Gruppen Zugriff auf ein Laufwerk, Gerät oder eine Anwendung erhalten.



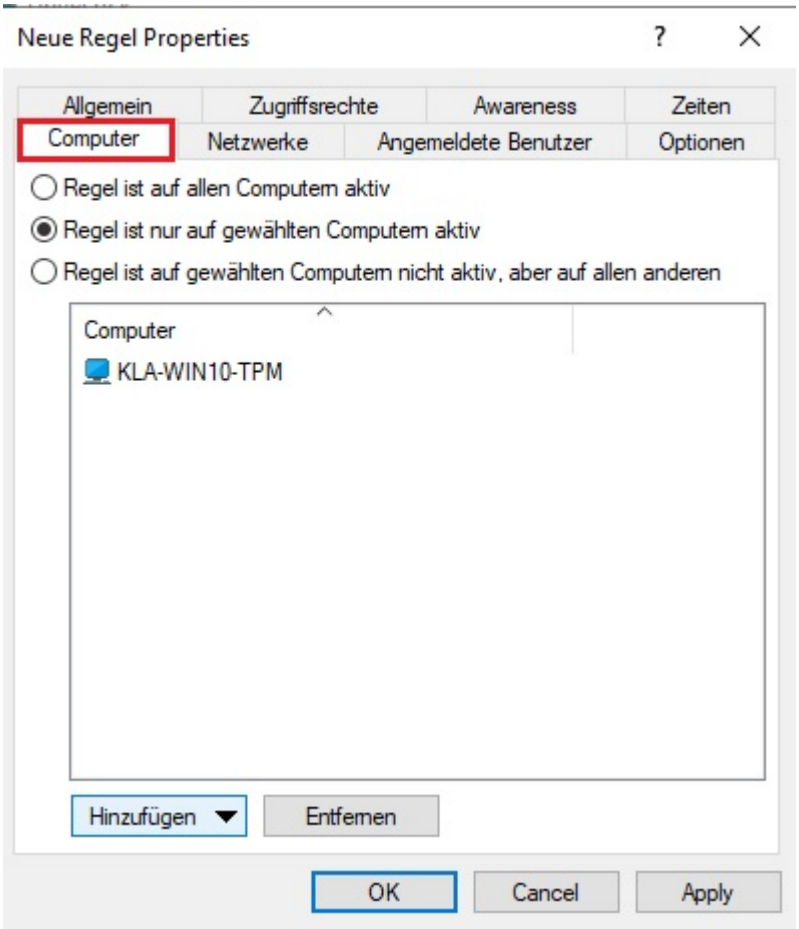
Folgende Möglichkeiten stehen zur Auswahl:

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

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

5.4.2.3 Einschränkungen für Computer

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



Wählen Sie eine der folgenden Möglichkeiten:

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

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

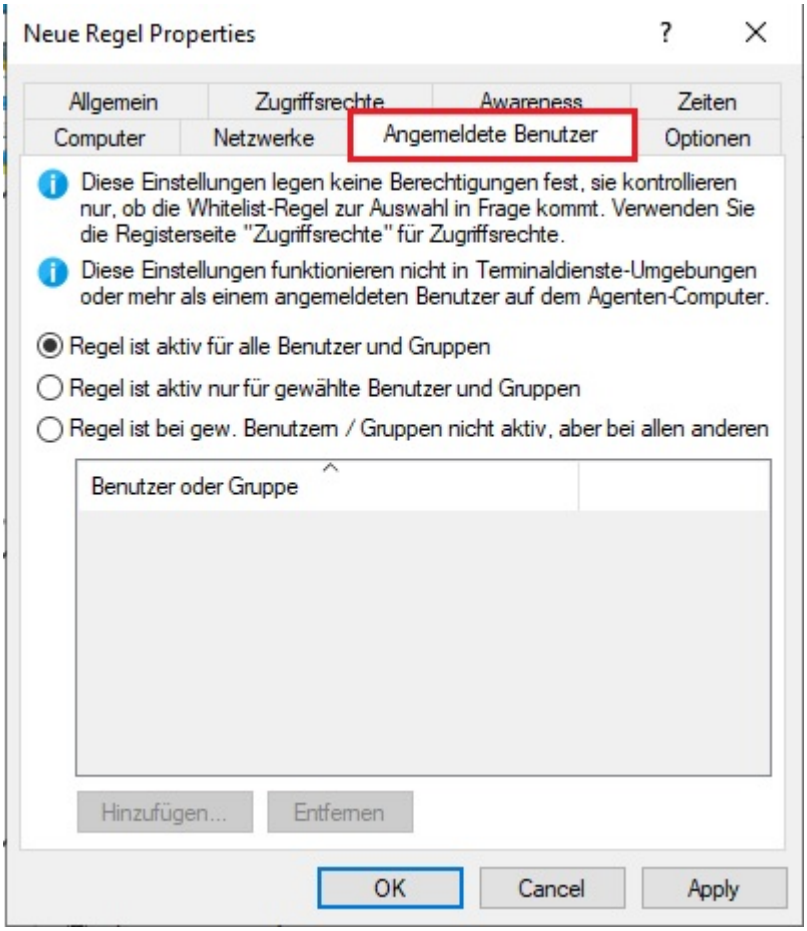
Durch **Entfernen** werden zuvor ausgewählte Computer aus der Liste gelöscht.

5.4.2.4 Einschränkungen für angemeldete Benutzer

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

Die Benutzer- und Gruppenprüfung ist nicht zu verwechseln mit den Berechtigungen, welche über den Reiter **Zugriffsrechte** konfiguriert werden. Diese Prüfung bestimmt lediglich, ob diese Regel für den gerade angemeldeten Benutzer überhaupt in Betracht gezogen wird.

Erst in diesem Fall wird der Zugriff entsprechend der gesetzten Berechtigungen erlaubt bzw. verweigert.



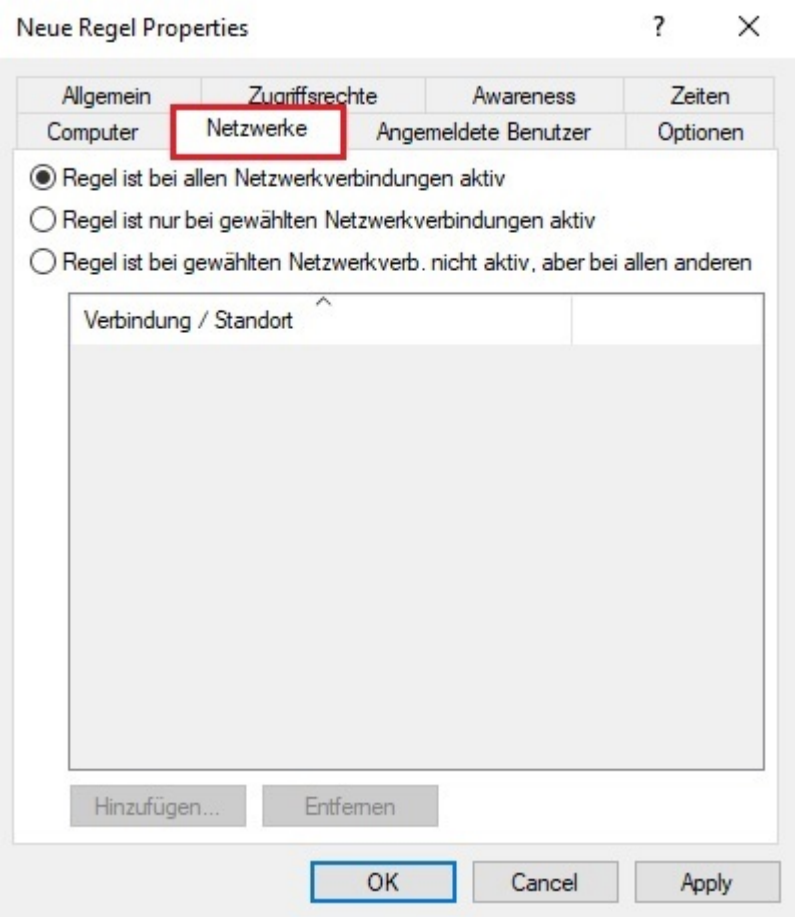
Wählen Sie eine der folgenden Möglichkeiten:

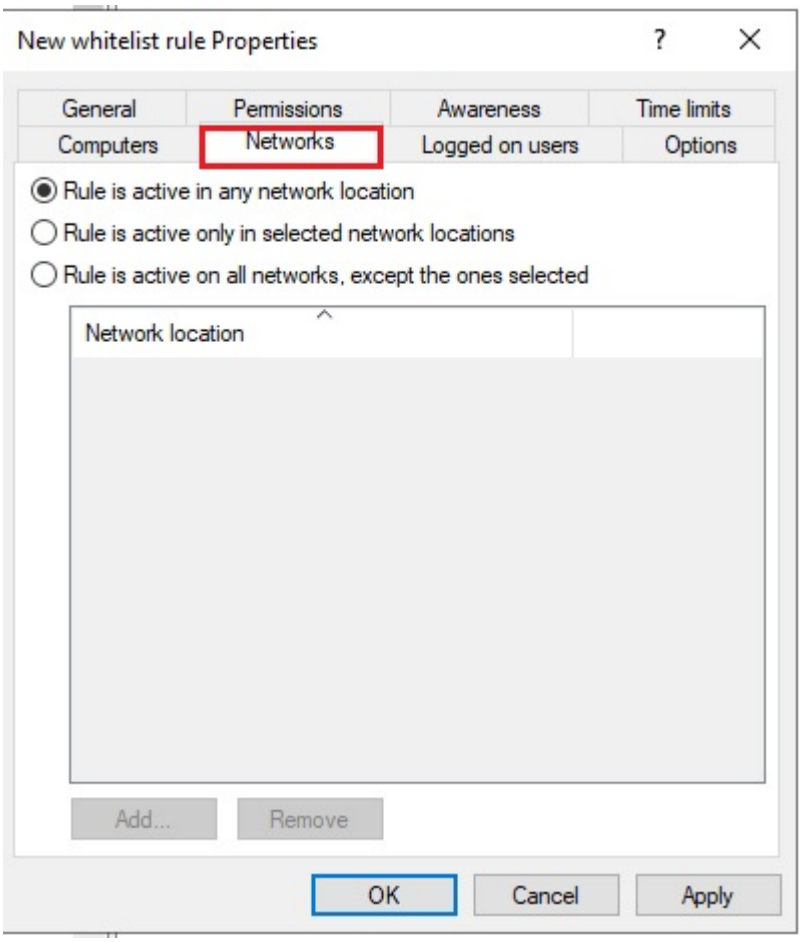
- Die Regel gilt für alle Benutzer
- Die Regel gilt nur für die aufgelisteten Benutzer bzw. Gruppen
- Die Regel gilt für alle außer den aufgelisteten Benutzer bzw. Gruppen

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

5.4.2.5 Netzwerkprofile

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


Neue Regel Properties
Allgemein
Zugriffsrechte
Awareness
Zeiten
Computer
Netzwerke
Angemeldete Benutzer
Optionen
Regel ist bei allen Netzwerkverbindungen aktiv
Regel ist nur bei gewählten Netzwerkverbindungen aktiv
Regel ist bei gewählten Netzwerkverb. nicht aktiv, aber bei allen anderen
Verbindung / Standort
Hinzufügen...
Entfernen
OK
Cancel
Apply



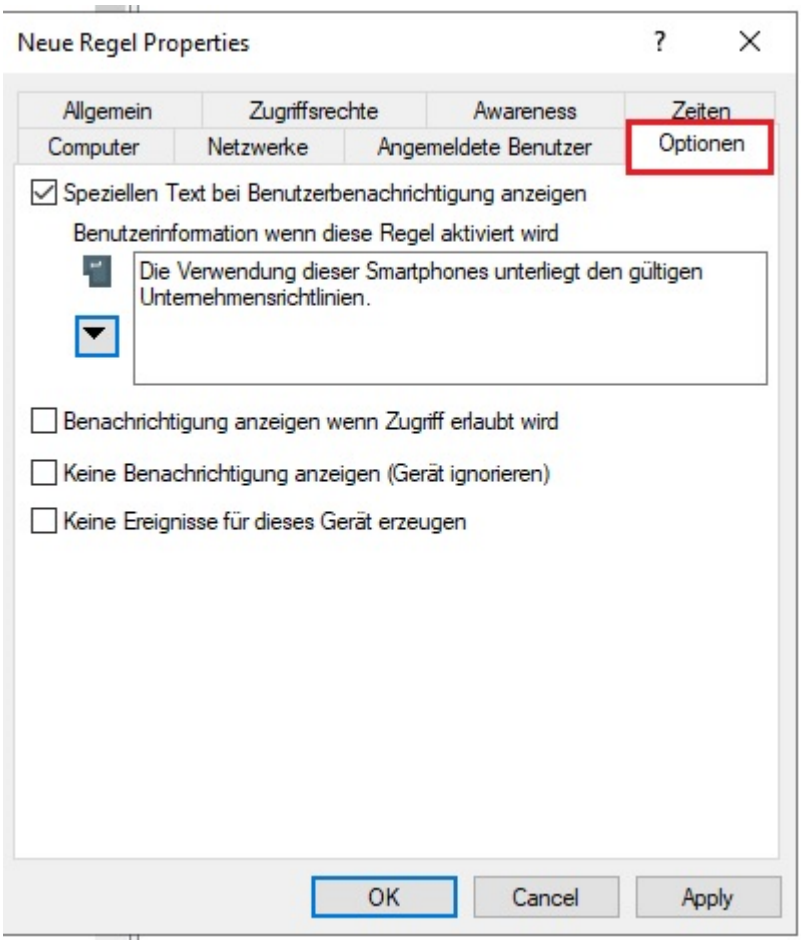
Wählen Sie eine der folgenden Möglichkeiten:

- 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.

5.4.2.6 Optionen

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



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

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

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

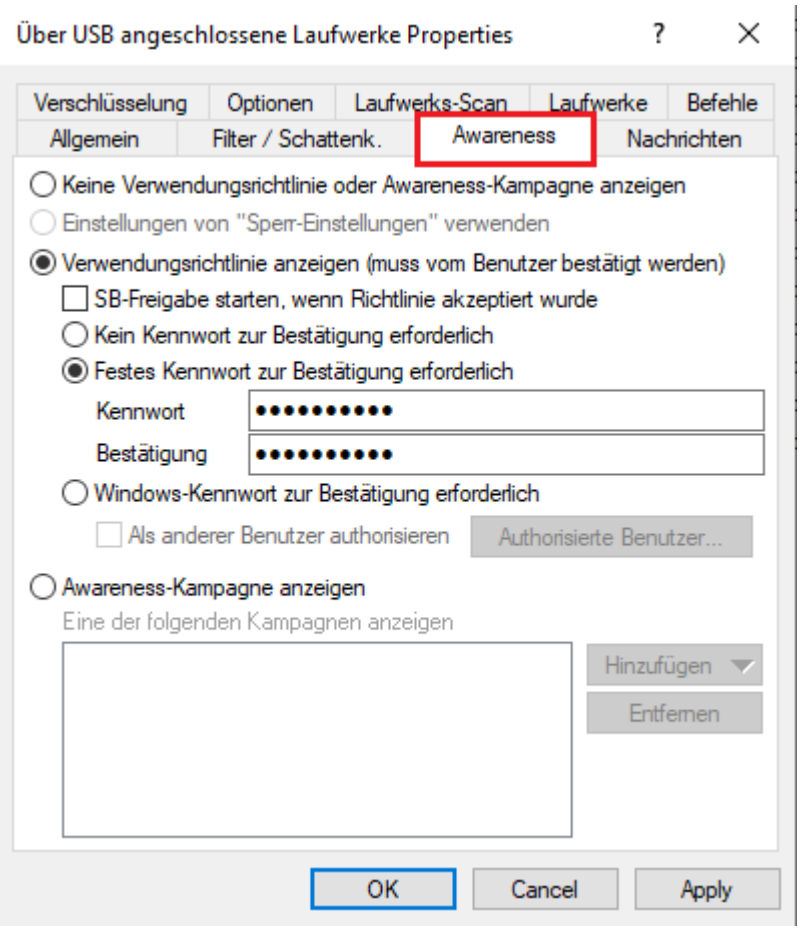
Diese sprachabhängige Meldung wird durch ein Sprechblasen-Symbol an der linken oberen Ecke des Eingabefeldes dargestellt.

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

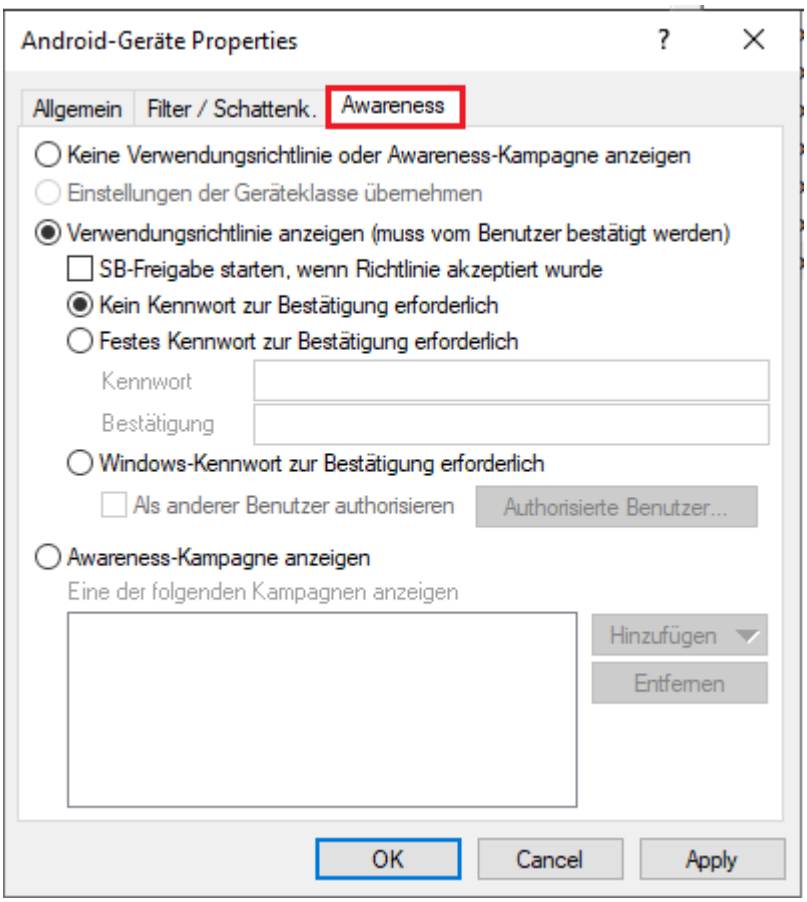
Wenn Sie die Erzeugung von Überwachungsereignissen für diese Whitelist-Regel unterdrücken wollen, markieren Sie bitte **Keine Ereignisse für dieses Gerät erzeugen**.

5.4.2.7 Awareness

Auf dem Reiter **Awareness** können Sie eine Verwendungsrichtlinie global für die gesamte Richtlinie erstellen. Aktivieren können Sie diese dann ähnlich wie eine Security Awareness Kampagne innerhalb einer Laufwerksregel



oder einer Geräteregel:



Wählen Sie dazu die Option **Verwendungsrichtlinie anzeigen (muss vom Benutzer bestätigt werden)**.

Folgende Optionen stehen Ihnen noch zur Verfügung:

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

- Awareness-Kampagne anzeigen: Informationen zum Einsatz von Awareness-Kampagnen finden Sie in der entsprechenden Dokumentation auf DriveLock Online Help.

5.5 Anwendungen / Application Control

Die Beschreibung dieses DriveLock-Moduls finden Sie in der Application Control Dokumentation auf DriveLock Online Help.

5.6 Verschlüsselung

Die Themen DriveLock Disk Protection, BitLocker Management, Encryption 2-Go und BitLocker To Go, sowie DriveLock Pre-Boot-Authentifizierung werden in der DriveLock Encryption Dokumentation erläutert. Das Thema File Protection ist derzeit in Überarbeitung und noch im DriveLock Administrationshandbuch enthalten. Sie finden beides auf DriveLock Online Help.

5.7 Defender Management

Die Beschreibung dieses DriveLock-Moduls finden Sie in der Defender Management Dokumentation auf DriveLock Online Help.

5.8 Security Awareness

Die Beschreibung des DriveLock-Moduls finden Sie in der Security Awareness Dokumentation auf DriveLock Online Help.

5.9 Inventarisierung und Schwachstellenscan

Die Beschreibung der Themen Inventarisierung, Client Compliance und Schwachstellenscan finden Sie in der Vulnerability Scanner Dokumentation auf DriveLock Online Help.

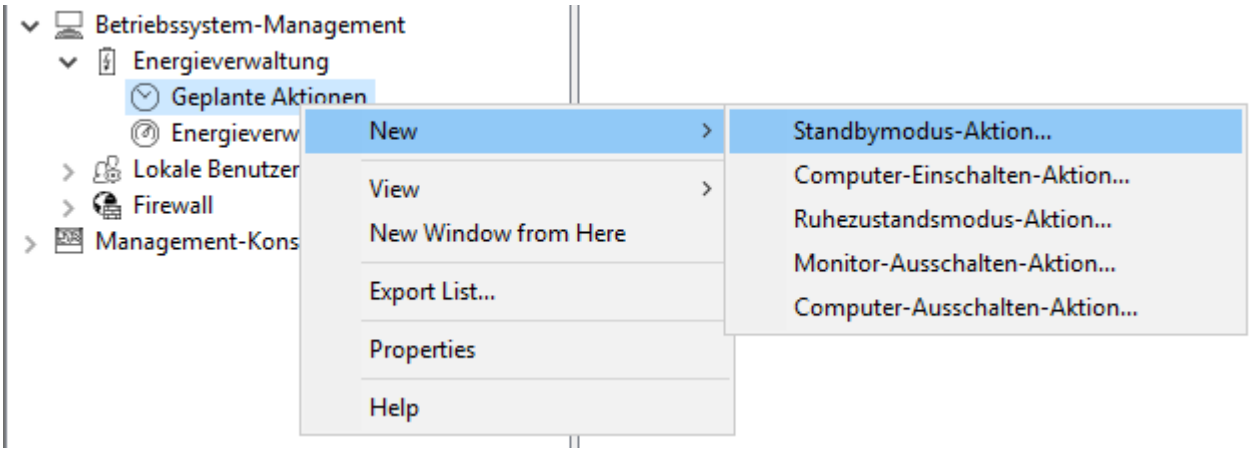
5.10 Betriebssystem-Management

In diesem Abschnitt konfigurieren Sie Einstellungen für die Betrieb und das Systemmanagement der DriveLock Agenten.

5.10.1 Energieverwaltung

In einer DriveLock Richtlinie können Sie Aktionen planen, wenn Rechner im Standbymodus sind, pausieren oder sich aus- oder einschalten sollen oder wann welcher Windows Energiesparplan gelten soll.

Wählen die gewünschte Aktion oder den passenden Plan.



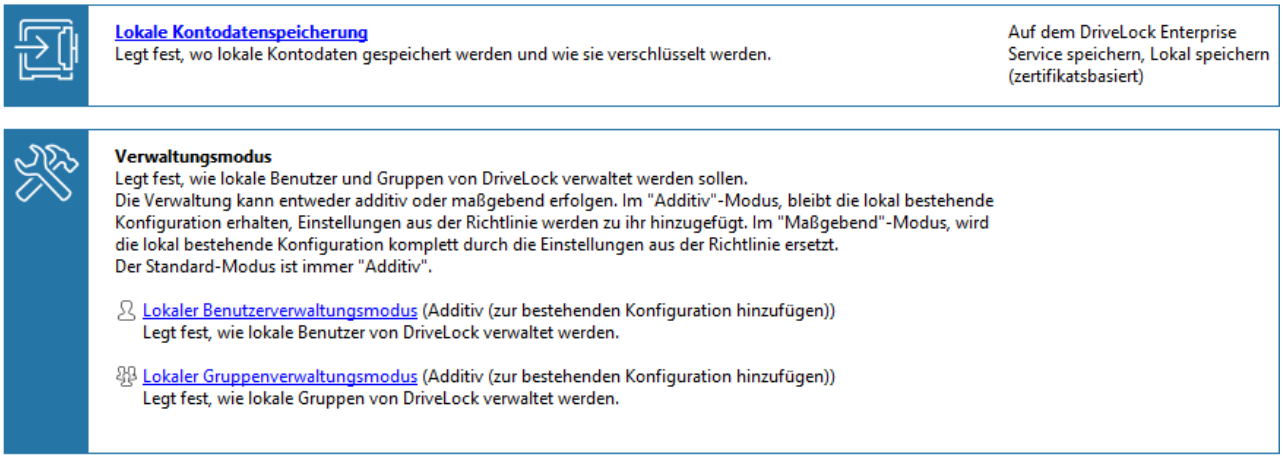
5.10.2 Lokale Benutzer und Gruppen

Mit dieser DriveLock-Funktionalität können Sie wichtige Zugriffsrechte für bestimmte Benutzer und Gruppen einschränken und somit Ihre Zero-Trust-Strategie leichter umsetzen.

Beispielsweise können bestimmte Benutzer der Gruppe der lokalen Administratoren hinzugefügt werden, um somit verschiedene lokale Administratoren für eine bestimmte Gruppe von Computern zu haben. Sie geben dann an, welcher Benutzer lokale Admin-Rechte auf welchen Systemen bekommt.

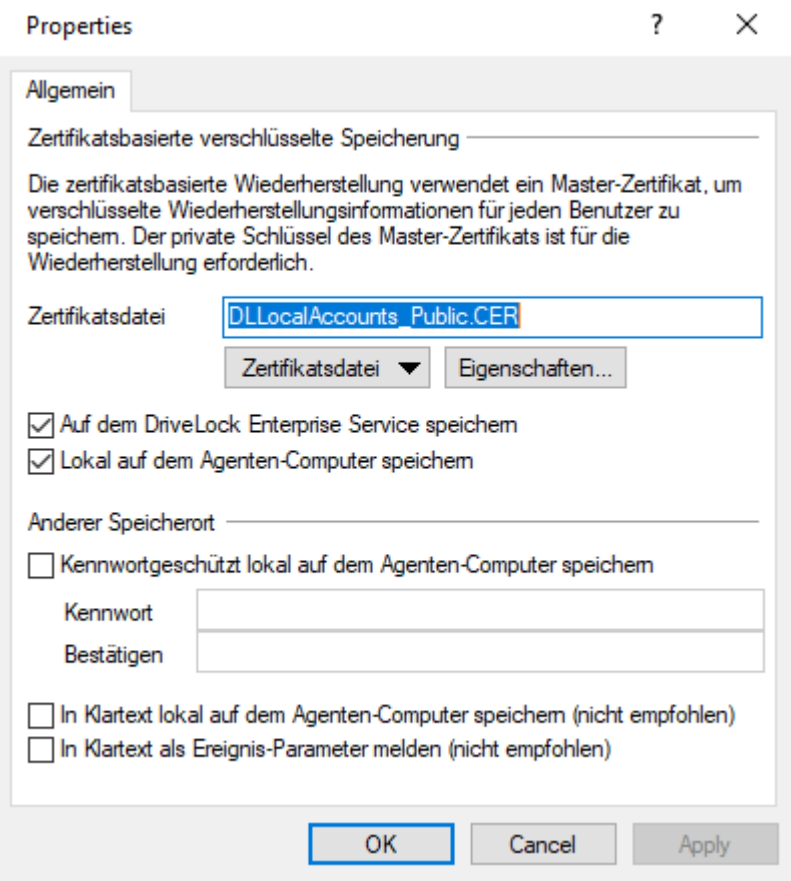
5.10.2.1 Einstellungen

Folgende Einstellungen sind möglich:



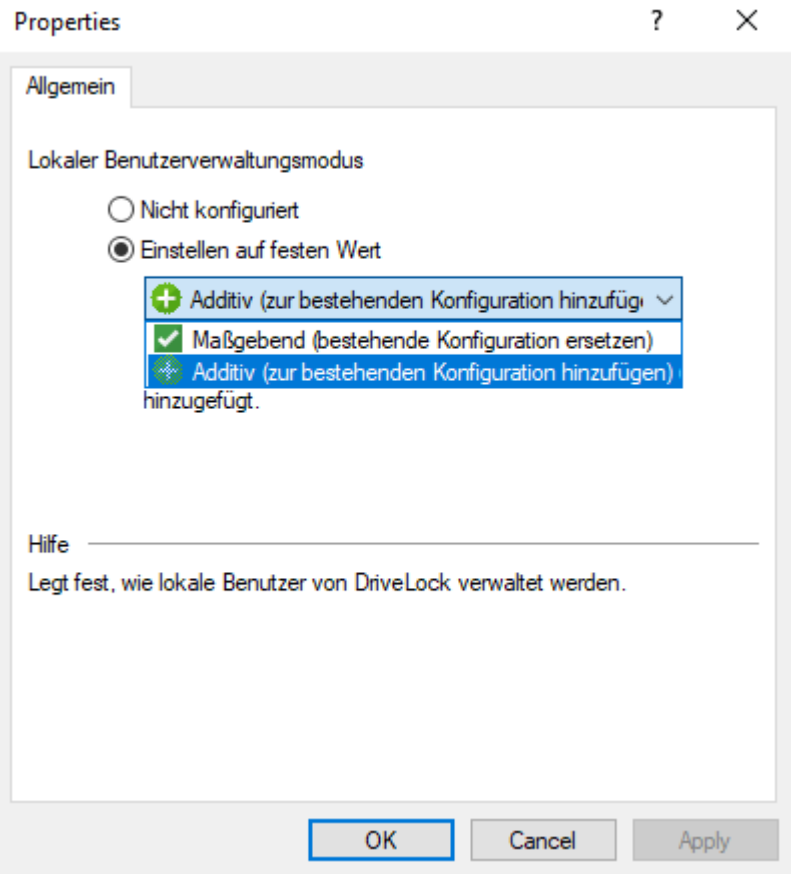
Lokale Kontodatenspeicherung

Mit dieser Einstellung können Sie festlegen, wo Benutzernamen und Kennwörter gespeichert werden - Zertifikatsbasiert lokal oder auf dem DES.



Einstellungen zum Verwaltungsmodus

Lokaler Benutzerverwaltungsmodus:



Über den **Benutzer- und Gruppenverwaltungsmodus** kann definiert werden, wie Benutzer und Gruppen von DriveLock verwaltet werden.

- Im additiven Modus (Standard) werden die vorhandenen lokalen Benutzer nicht verändert, außer den in der Richtlinie definierten Benutzern. Wenn also z.B. ein Benutzer in der Richtlinie existiert, wird dieser Benutzer zusätzlich zu allen anderen lokalen Benutzern hinzugefügt.
- Im maßgebenden Modus werden die vorhandenen lokalen Benutzer/Gruppen alle gelöscht und nur die in der Richtlinie definierten Benutzer bzw. Gruppen erstellt.

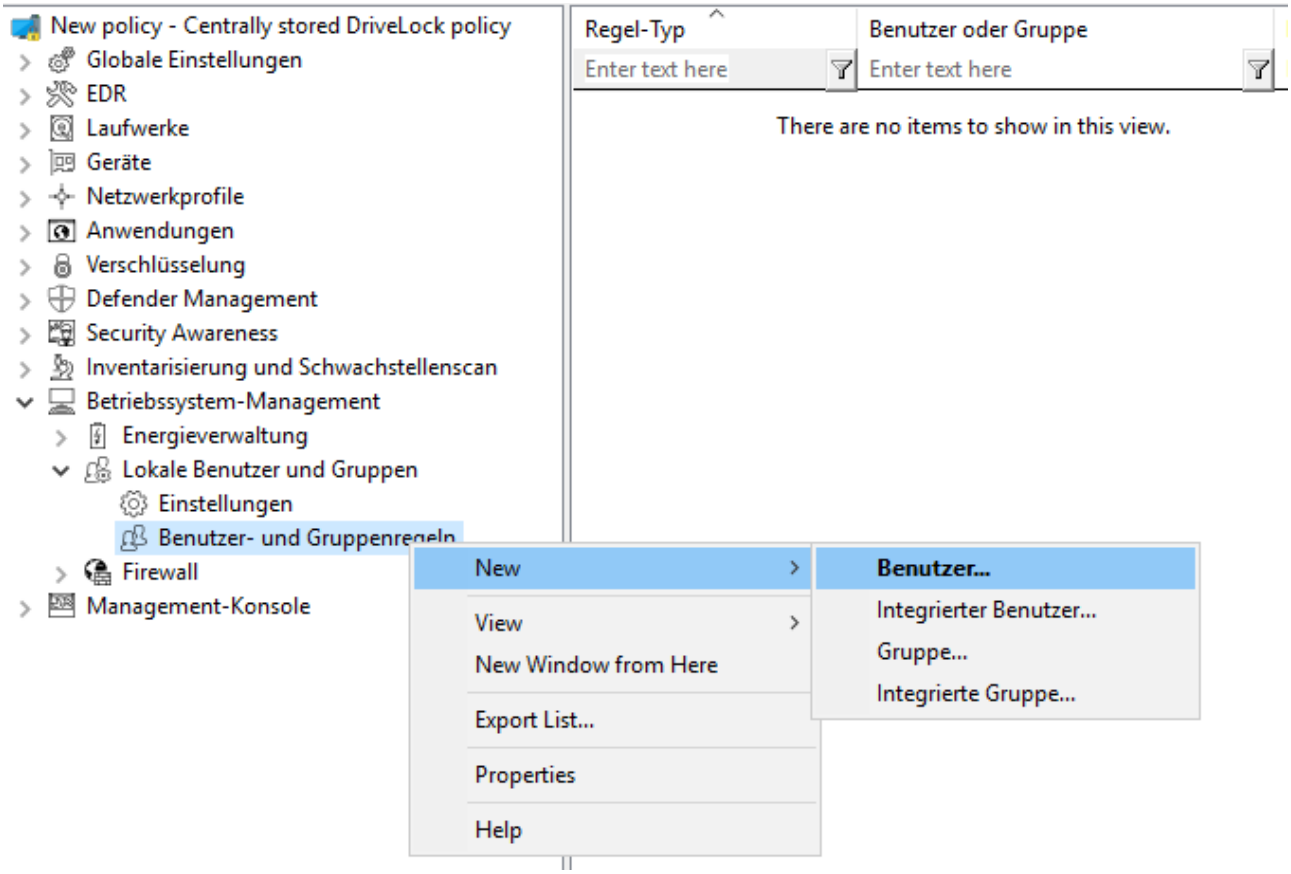
5.10.2.2 Benutzer- und Gruppenregeln

Setzen Sie Benutzer- und Gruppenregeln für die Verwaltung lokaler Benutzer und Gruppen ein. Je nach Verwaltungsmodus können in DriveLock definierte Benutzer und Gruppen zur lokalen Benutzerdatenbank hinzugefügt werden oder sie ersetzen die Benutzer und Gruppen in der lokalen Benutzerdatenbank vollständig.

Benutzerregeln

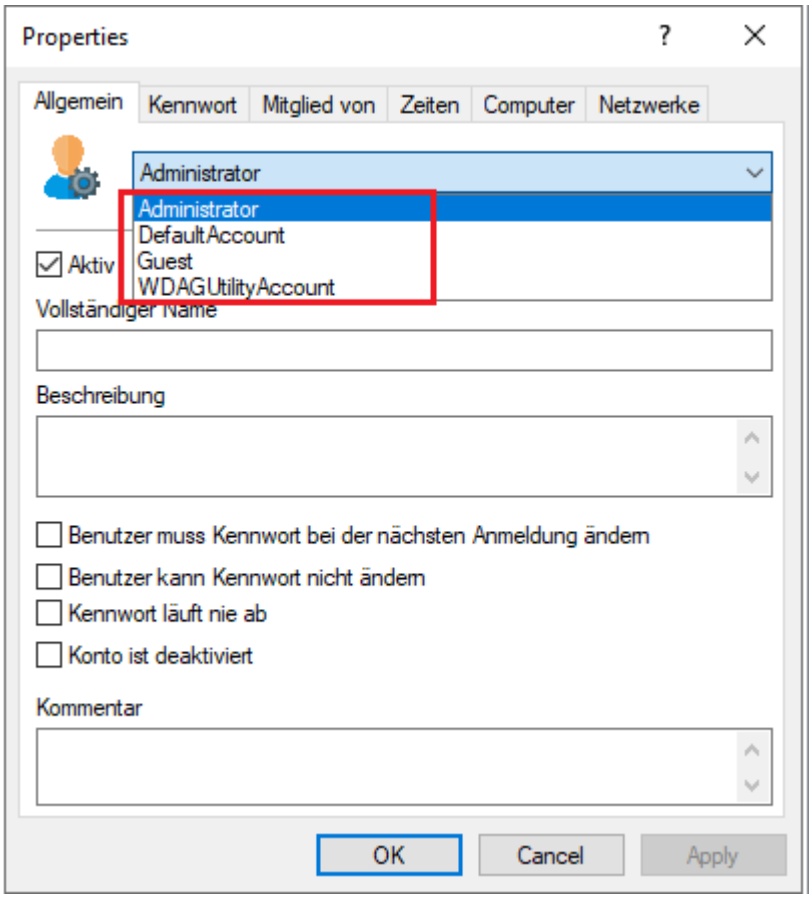
Für jeden Benutzer kann eine Regel erstellt werden.

Gehen Sie wie in der Abbildung gezeigt vor:

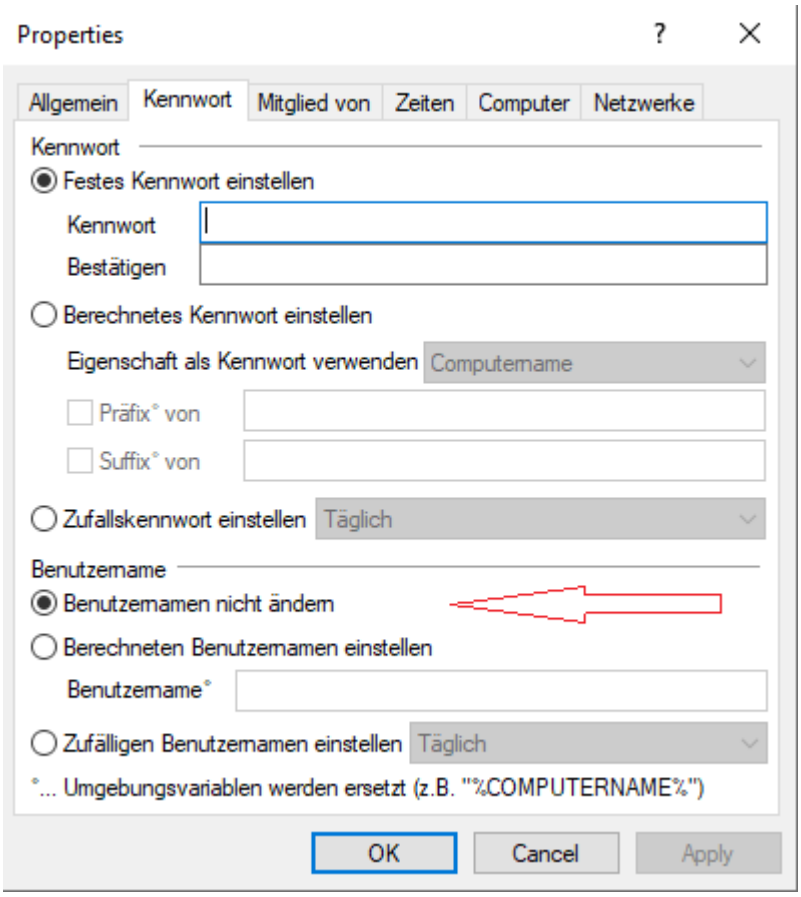


Der Unterschied zwischen integrierten und benutzerdefinierten Konten besteht im Benutzernamen.

Die integrierten Konten sind die vier Konten, die bei der Windows-Installation angelegt werden (am wichtigsten das "Administrator"-Konto). Diese können nicht gelöscht werden, können aber in der Regel umbenannt werden.



Auf dem Reiter **Kennwort** geben Sie an, ob ein festes, ein errechnetes oder ein zufallsgeneriertes Kennwort für das Konto verwendet werden soll. Außerdem können Sie bei integrierten Benutzern angeben, ob der feste Benutzername geändert werden soll:



Gruppenregeln

Auch hier sind die eingebauten Gruppen die vordefinierten Windows-Gruppen. In den Regeln wird die Mitgliedschaft definiert.

Andere Benutzer oder AD-Benutzer/Gruppen können hinzugefügt (über die Schaltfläche **Einschließen**) oder aus der Gruppe entfernt werden (über die Schaltfläche **Ausschließen**). Wenn Sie also z. B. eine bestimmte AD-Gruppe aus der Gruppe "Administratoren" entfernen möchten, erstellen Sie eine Regel für die eingebaute Gruppe und fügen der Regel ein "Ausschließen" hinzu.

5.10.2.2.1 Lokale Benutzerkonten abrufen

Kennwörter können mit Hilfe eines lokalen Assistenten abgerufen werden, der über den Menübefehl **Lokale Benutzerkonten abrufen...** auf dem DriveLock Agenten im Tray-Symbolmenü und/oder Startmenü zur Verfügung steht.

Im Assistenten werden Sie nach dem Benutzernamen (oder dem integrierten Benutzer, dessen Name geändert werden kann) und den Anmeldeinformationen gefragt und das Kennwort und der Benutzername angezeigt. Es werden nur die verfügbaren Optionen angezeigt, d. h. wenn Daten nur auf DES hochgeladen werden, ist die Option Kennwort ausgegraut.

In den Einstellungen für Taskbar-Informationsbereich können Sie angeben, dass der Menüeintrag **Lokale Benutzerkonten abrufen...** im Startmenü des Agenten angezeigt wird. Setzen Sie hierzu ein Häkchen bei **Verknüpfung zum Benutzerkonten-Abruf im Startmenü anzeigen**.

5.10.2.2.2 Lokale Benutzer und Gruppen in der Agenten-Fernkontrolle

In der Agenten-Fernkontrolle wurde eine Seite in den Agenteneigenschaften-Dialog eingefügt, die die lokalen **Benutzer und Gruppen** anzeigt. Die von DriveLock verwalteten Benutzer/Gruppen werden mit einem farbigen Symbol angezeigt, während andere Benutzer/Gruppen in Graustufen dargestellt werden. Ein Klick auf Details zeigt detaillierte Informationen über den Benutzer/die Gruppe an.

5.10.3 Firewall

Mit diesen Optionen können die Firewall-Einstellungen für DriveLock Agenten verwaltet werden. Es lassen sich dadurch Regeln für eine bestimmte Gruppe von Computern konfigurieren. DriveLock erweitert die eingebaute Funktionalität der Windows Firewall durch dynamisches Hinzufügen und Entfernen von Regeln auf Basis von bedingten Einstellungen.

5.10.3.1 Einstellungen

Folgende allgemeine Einstellungen sind möglich:

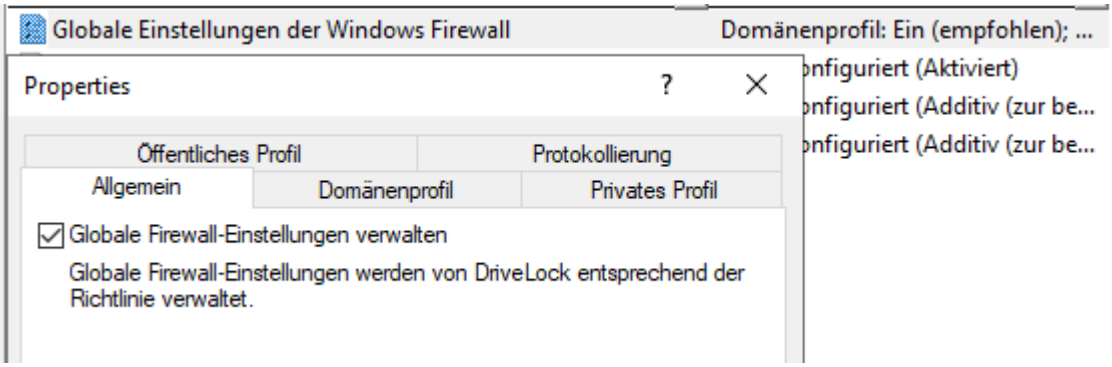
Steuerung von Windows Firewall aktivieren/deaktivieren:

Um die Steuerung der Windows Firewall auf DriveLock Agenten zu ermöglichen, muss diese Einstellung aktiviert sein. Dies ist standardmäßig der Fall. DriveLock kann somit

Einstellungen an der Firewall vornehmen, Regeln verwalten und die Firewall betreffende Ereignisse erzeugen.

Globale Einstellungen der Windows Firewall:

In den globalen Einstellungen können Sie entscheiden, ob DriveLock die allgemeinen Einstellungen der Windows Firewall verwalten soll. Außerdem können Sie die Firewall-Einstellungen für jeden Netzwerktyp festlegen und die Protokollierung konfigurieren.



- Reiter **Allgemein**: Wenn DriveLock die Windows Firewall entsprechend den Einstellungen in diesem Dialog vornehmen soll, aktivieren Sie Globale Firewall-Einstellungen verwalten. Diese Einstellung hat keinen Einfluss auf die Firewallregeln. Die Regeln werden entsprechend der Richtlinie verwaltet, selbst wenn die Einstellung deaktiviert ist.
- Reiter **Domänenprofil**, **Privates Profil** und **Öffentliches Profil**: Sie können die Firewall für jedes der Netzwerktypen separat konfigurieren oder nur die Konfiguration für das Domänenprofil vornehmen und die Einstellung **Diese Einstellungen auf alle Profile anwenden** aktivieren, wenn alle Profile gleich konfiguriert werden sollen.
  Folgende Optionen stehen zur Auswahl:
  - **Firewallstatus**: Wählen Sie aus, ob die Firewall für den gewählten Netzwerktyp aktiviert oder deaktiviert werden soll.
  - **Eingehende Verbindungen**: Wählen Sie aus, ob eingehende Verbindungen für den gewählten Netzwerktyp erlaubt oder blockiert werden sollen. Standardmäßig werden eingehende Verbindungen blockiert, wenn keine der definierten Regeln zutrifft.
  - **Ausgehende Verbindungen**: Wählen Sie aus, ob ausgehende Verbindungen für den gewählten Netzwerktyp erlaubt oder blockiert werden sollen. Standardmäßig werden ausgehende Verbindungen erlaubt, wenn keine der definierten Regeln zutrifft.

    - **Anzeigen von Benachrichtigungen an den Benutzer, wenn ein Programm vom Empfang eingehender Verbindungen blockiert wird**: Aktivieren Sie diese Einstellung, wenn der Benutzer eine Benachrichtigung erhalten soll, wenn die Firewall eine Verbindung blockiert, für die bisher keine Regel existiert. Standardmäßig sind die Benachrichtigungen aktiviert.
    - **Unicast-Antworten auf Multicast- oder Broadcast-Netzwerkverkehr zulassen**: Aktivieren Sie diese Einstellung, wenn Unicast-Antworten auf Multicast- oder Broadcast-Anfragen innerhalb von 3 Sekunden zugelassen werden sollen. Es wird empfohlen, diese Einstellung zu deaktvieren, um mögliche "Denial of service"-Angriffe zu vermeiden. Diese Einstellung hat keinen Einfluss auf DHCP. DHCP Unicast-Antworten werden von der Firewall immer zugelassen. Standardmäßig ist diese Einstellung aktiviert.
- Reiter **Protokollierung**: Hier können Sie die Protokollierungseinstellungen anpassen. Wählen Sie aus, welche Verbindungen protokolliert werden sollen.
  Folgende Optionen stehen zur Auswahl:
    - **Netzwerkverbindungen protokollieren**: Aktivieren Sie diese Einstellung, wenn die Netzwerkverbindungen protokolliert werden sollen. Der Standardpfad für das Protokoll lautet `%windir%\system32\logfiles\firewall\pfirewall.log`
    - **Erfolgreiche Verbindungen protokollieren**: Aktivieren Sie diese Einstellung, wenn erfolgreiche Verbindungen protokolliert werden sollen.
    - **Verworfene Verbindungen protokollieren**: Aktivieren Sie diese Einstellung, wenn verworfene Verbindungen protokolliert werden sollen.
    - **Multicast-Pakete bei der Protokollierung ignorieren**: Aktivieren Sie diese Einstellung, um Multicast-Pakete von der Protokollierung auszuschließen.
    - **Verbindungen mit folgenden Ports ignorieren**: Geben Sie hier Ports an, die von der Protokollierung ausgeschlossen werden sollen.

Verwaltungsmodus für ein- bzw. ausgehende Verbindungen:

Der Verwaltungsmodus legt fest, wie Firewallregeln von DriveLock verwaltet werden. Die Verwaltung kann entweder additiv oder maßgebend erfolgen.

- Im **Additiv**-Modus bleiben die lokal bestehenden Regeln erhalten. Die Regeln aus der Richtlinie werden nur hinzugefügt. Wenn die Richtlinie integrierte Firewallregeln enthält, die auf dem Agenten ebenfalls vorhanden sind, werden diese Regeln entsprechend der Richtlinie modifiziert.

- Im **Maßgebend**-Modus werden vorhandene Regeln auf dem Agenten gelöscht und durch die Regeln in der Richtlinie ersetzt. Vorhandene integrierte Regeln auf dem Agenten werden von DriveLock nur deaktiviert und nicht gelöscht, wenn sie in der Richtlinie nicht vorhanden sind.

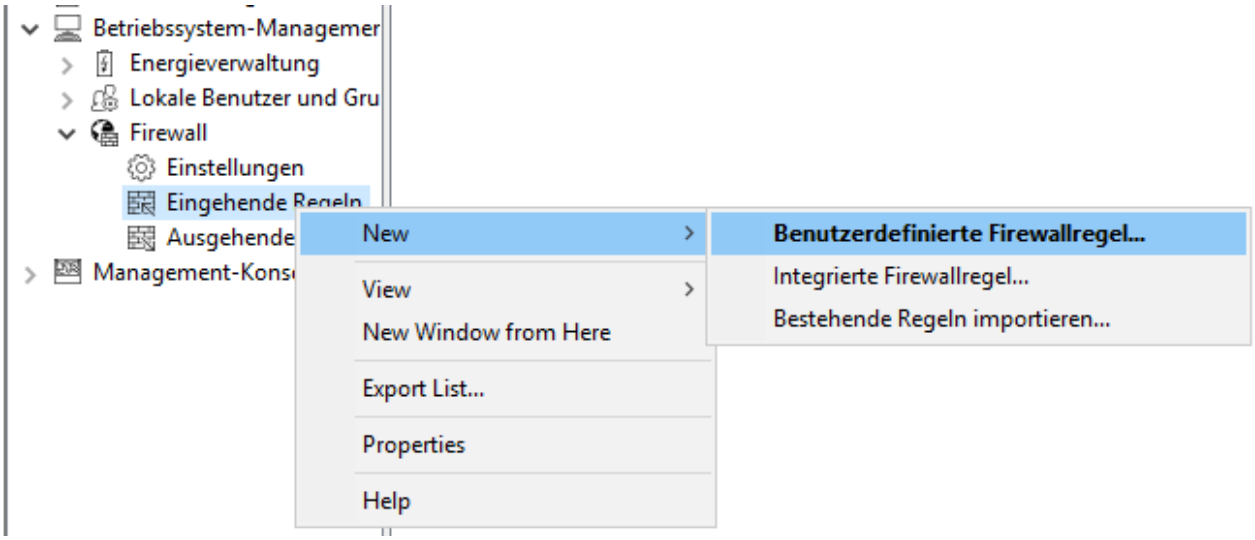
Regeln, die über die Gruppenrichtlinie angelegt wurden, bleiben weiterhin bestehen. Sie werden von DriveLock weder modifiziert noch gelöscht.

Regeln, die von DriveLock selbst für die Produktfunktionalität angelegt werden, sind von der Verwaltung ausgeschlossen. Sie werden immer angelegt und bleiben auch im maßgebenden Modus erhalten.

Die Standardeinstellung ist additiv.

5.10.3.2 Ein- und ausgehende Regeln

In der Richtlinie sind haben Sie die Möglichkeit, ein- und ausgehende Regeln zu definieren. Wählen Sie dafür **Eingehende Regeln** oder **Ausgehende Regeln** aus und öffnen Sie das Kontextmenü.



Folgende Konfigurationsoptionen stehen zur Verfügung:

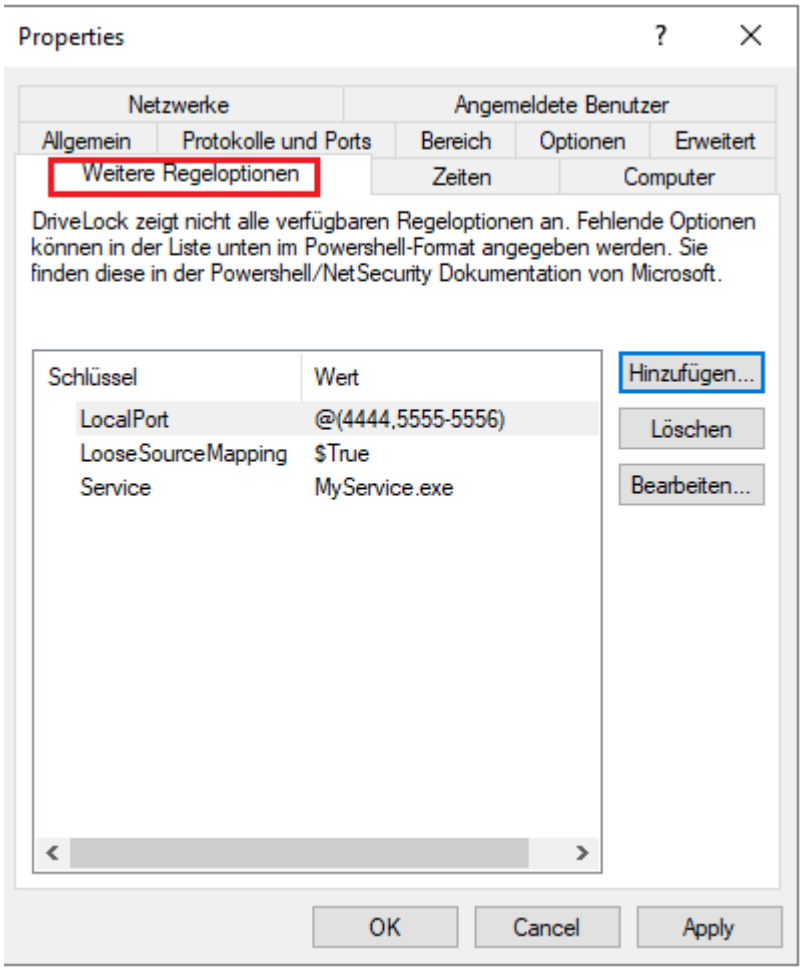
- **Benutzerdefinierte Firewallregel**:
  1. Geben Sie den Namen der Regel und eine Beschreibung an.
  2. Wählen Sie bei der Aktion aus, ob die Verbindung blockiert oder zugelassen werden soll.
  3. Wählen Sie aus, ob die Regel in der DriveLock-Richtlinie aktiv sein soll. Wenn Sie diese Option abwählen, wird die Regel so behandelt, als ob sie in der Richtlinie nicht existieren würde.

4. Wählen Sie aus, ob die Regel in der Windows Firewall als aktiviert oder deaktiviert angelegt werden soll.
5. Diese beiden Einstellungen können Sie später im Kontextmenü der Regel setzen, ohne den Eigenschaftendialog wieder öffnen zu müssen.
6. Definieren Sie danach die restlichen Optionen der Regel.

Wenn Sie eine Option benötigen, die in den Dialogseiten nicht vorhanden ist, haben Sie die Möglichkeit, diese Option auf dem Reiter **Weitere Regeloptionen** hinzuzufügen. Nutzen Sie dafür das Powershell-Format. Eine Liste der möglichen Optionen finden Sie in der Powershell/NetSecurity Dokumentation über die Befehle `New-NetFirewallRule` und `Set-NetFirewallRule` von Microsoft.
Beachten Sie bitte folgenden Syntaxregeln:

- Als Schlüsselname wird der Name der Option angegeben.
- Als Wert kann ein String, ein Boolean-Wert oder eine Liste angegeben werden.
- Für Optionen vom Typ String geben Sie einfach den Wert ein.
- Für Optionen vom Typ Boolean können die Werte `$True` oder `$False` verwendet werden.
- Für Optionen, die eine Liste aus Strings erwarten, geben Sie die Werte in Klammern mit einem `$`-Zeichen davor an. Das gilt auch, wenn die Liste nur einen Wert enthalten soll, z.B. `$(Wert1, Wert2)`.

Im Beispiel können Sie mit der Option **Service** den Dienst angeben, für den die Regel gelten soll (siehe Abbildung):



Hinweis: Beachten Sie, dass diese Optionen erst ab Windows 8.1 funktionieren. Auf älteren Betriebssystemen werden diese Optionen ignoriert.

- **Integrierte Firewallregel**:
  Integrierte Firewallregeln sind vordefinierte Firewallregeln, die in das Betriebssystem integriert sind. Wenn Sie eine integrierte Firewallregel in der Richtlinie anlegen, wird die entsprechende Regel auf dem Agenten modifiziert. Wenn die Regel auf dem Agenten noch nicht existiert, wird sie angelegt.
  Bei der Auswahl der Regel haben Sie die Möglichkeit, die Regel aus Ihrer lokal vorhanden Regelliste auszuwählen, oder sich die Liste von einem Agenten anzeigen zu lassen.

Hinweis: . Beachten Sie, dass nicht jede Regel auf jedem Betriebssystem existiert.

Gehen Sie weiter vor wie beim Anlegen der benutzerdefinierten Regeln.

- **Bestehende Regeln importieren**:
  Sie können alle bestehenden Firewallregeln auf einmal importieren. Auch hier gibt die Wahl, die lokal vorhanden Regeln, also die Regeln des Computers, auf dem der Richtlinien Editor gerade läuft, oder die Regeln von einem Agenten zu verwenden.
  Es kann vorkommen, dass die zu importierende Regeln Optionen enthalten, die von DriveLock nicht importiert werden können oder in der Richtlinie Regeln mit gleichem Namen bereits existieren. In diesem Fall wird im Import-Dialog ein Hinweis angezeigt und eine Datei im `%temp%`-Verzeichnis erzeugt, die eine Liste dieser Regeln enthält.
  1. Klicken Sie auf **Details anzeigen**, um zum Verzeichnis zu navigieren.
  2. Öffnen Sie die Datei `LocalFirewallImportReport.txt` für lokale Regeln oder `RemoteFirewallImportReport.txt` für Regeln des gewählten Agenten.
  3. Wählen Sie aus, ob die importierten Regeln zu den bestehenden Regeln in der Richtlinie hinzugefügt werden oder sie ersetzen sollen.
  4. Klicken Sie **Importieren**, um die Regen zu importieren. Dieser Vorgang kann einige Minuten dauern. Nach dem Import enthält die Spalte **Bemerkung** das Datum und den Namen des Computers, von dem die Regeln importiert wurden.
  5. Nach dem Import können Sie Regeln wie gewohnt bearbeiten.

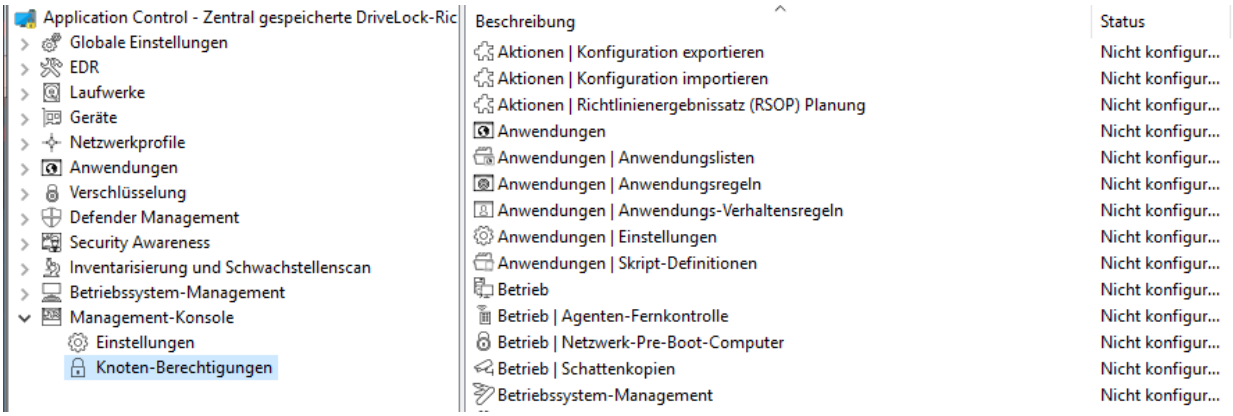
Hinweis: Beachten Sie, dass bei den integrierten Firewallregeln manche Optionen schreibgeschützt sind und nicht geändert werden können.

5.11 Management-Konsole

In diesem Abschnitt können Sie spezielle Management-Konsolen-Richtlinien festlegen, insbesondere Berechtigungen für die Benutzung der Konsole.

5.11.1 Knoten-Berechtigungen

Die DMC kann so konfiguriert werden, dass bestimmte Benutzer oder Gruppen nur bestimmte Funktionen ausführen dürfen. Es ist für fast jeden Punkt in der Navigationskonsole möglich, Berechtigungen für Benutzer zu vergeben.

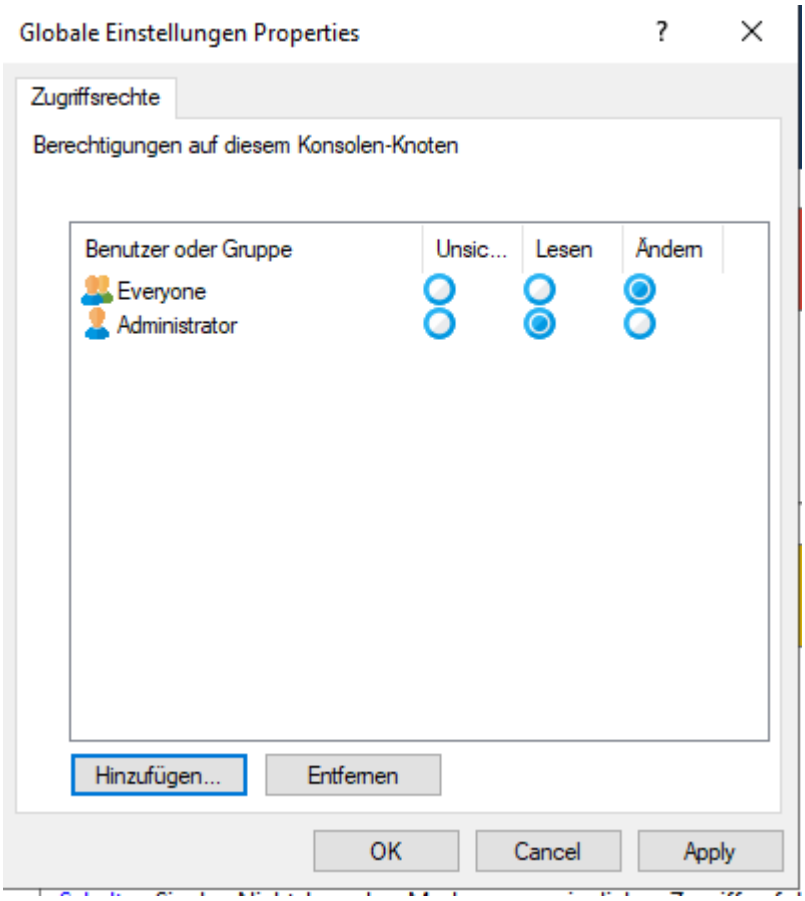


Die Konfiguration der Berechtigungen erfolgt innerhalb einer DriveLock Richtlinie als Einstellung für den DriveLock Agenten und nicht für eine DriveLock Management Konsole selbst. Damit wird sichergestellt, dass ein Anwender sich nicht auf seinem Rechner im Unternehmen eine DriveLock Management Konsole installieren und damit unbefugt arbeiten kann.

Der Abschnitt „Verteilung der DriveLock Konfigurationseinstellungen“ beschreibt die Möglichkeiten und die Verwendung von DriveLock Richtlinien.

Klicken Sie innerhalb der DriveLock Richtlinie auf den Punkt Management-Konsole -> Knoten-Berechtigungen, um alle aktuellen Knoten-Berechtigungen anzuzeigen. Nach der Installation bleiben alle Punkte im Zustand “Nicht konfiguriert”, solange bis eine Einstellung geändert wird. Standardmäßig hat die Gruppe “Jeder” Vollzugriff auf alle Punkte.

Klicken Sie doppelt auf ein Objekt, um dessen detaillierte Einstellungen anzusehen.



Klicken Sie auf Hinzufügen, um einen neuen Benutzer oder Gruppe diesem Knoten zuzuweisen. Wählen Sie eine Gruppe oder Benutzer und klicken auf Entfernen, um das ausgewählte Konto aus der Liste zu entfernen.

Es gibt folgende Knotenberechtigungen:

- Unsichtbar: Der Knoten ist für den Benutzer nicht sichtbar (und somit auch nicht zugreifbar)
- Lesen: Der Benutzer kann den Knoten benutzen, um sich alle aktuellen Einstellungen anzeigen zu lassen, kann aber nichts verändern
- Ändern: Der Benutzer kann alle Einstellungen innerhalb dieses Knotens verändern.

Wenn Sie verschiedene Berechtigungen für mehr als eine Gruppe vergeben und ein Benutzer ist in mehrere dieser Gruppen, dann wird die höher priorisierte Berechtigung angewendet. Wenn ein Benutzer zum Beispiel sowohl das Recht „Lesen“ als auch das Recht „Ändern“ hat, dass wird die Berechtigung „Ändern“ angewendet (analog zu den Berechtigungen in Windows).

Achtung: Es ist nicht möglich, irgendeinen Knoten ohne wenigsten einen Benutzer oder Gruppe zu konfigurieren, die Änderungs-Rechte haben. In diesem Fall wird eine Warnung angezeigt.

6 Problembehebung

Ein Kommandozeilen-basiertes Diagnose-Werkzeug steht Ihnen als Teil der kompletten DriveLock Installation zur Verfügung. Mit diesem Tool können Sie Speichergeräte auf einem Computer diagnostizieren.

Das Kommandozeilen-Programm “dlcmd.exe” wird in das DriveLock Installationsverzeichnis installiert. DlCmd.exe kann verschiedene Typen von Diagnose-Informationen anzeigen.

> Hinweis: Weitere Informationen zur Problembehebung finden Sie in den Knowledge Base Artikeln KBA00106: Sammeln und Übermittlung von Diagnosedaten vom DriveLock Agent - Trace (DriveLock Support Companion) und KBA00422: Sammeln von Diagnoseinformationen. Bei Fragen wenden Sie sich bitte an den DriveLock Support.

6.1 Agentenstatus überprüfen

Es gibt zwei Möglichkeiten, wie Sie als Administrator oder auch als Endbenutzer auf dem Computer mit DriveLock Agenten Informationen zum aktuellen Status des Agenten und seiner Konfiguration erhalten können:

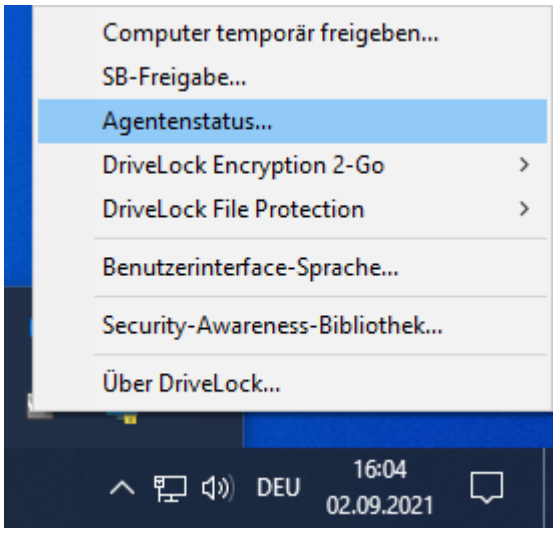
1. **Kommandozeilenbefehl**

   Öffnen Sie ein Kommandozeilenfenster und geben Sie `drivelock -showstatus` ein:

```
Microsoft Windows [Version 10.0.19042.630]
(c) 2019 Microsoft Corporation. Alle Rechte vorbehalten.

C:\Users\DLAdmin>drivelock -showstatus


---------------------------------------------------------------------
DriveLock Agent - Command line mode
---------------------------------------------------------------------

Agent identity
==============
Agent version:        2021.1 (21.1.2.34715)
Computer name:
Computer GUID:        {                    -4ab8-97f8-7ce69013e8e7}
Domain DNS name:      D
ActiveDirectory site: D                    st-Site-Name
Logged-on user name:  D
Logged-on user SID:

Component licensing status
==========================
Device control:         Licensed
Application control:    Licensed
Application behavior:   Licensed
Security awareness:     Licensed
Encryption 2-Go:        Licensed
File Protection:        Licensed
BitLocker management:   Licensed
BitLocker PBA option:   Licensed
BitLocker To Go:        No
Disk Protection:        No
Legacy OS option:       No
Vulnerability scan:     Licensed
                        With standard vulnerability catalog
Windows Defender:       Licensed
Native Security:        No
EDR:                    Licensed

Current agent status
====================
Environment:          Production
FDE special config:   No
Appl. terminal srv.:  No
Reboot pending:       No
Temporary unlock:     Not active
Policy config source: Not available (NoStore)
```

Sie erhalten detaillierte Informationen zu den Lizenzen, der Konfiguration und dem Status de einzelnen Komponenten.

2. Über das Tray-Icon auf dem DriveLock Agenten:



Wählen Sie **Agentenstatus...** aus.

Es öffnet sich ein neues Fenster, dort werden ebenfalls detaillierte Informationen in der gleichen Form angezeigt:

Status

```
Agent identity
==============
Agent version:          2021.1 (21.1.2.34715)
Computer name:          [redacted]
Computer GUID:          [redacted]
Domain DNS name:        [redacted]
ActiveDirectory site:   [redacted]
Logged-on user name:    [redacted]
Logged-on user SID:     [redacted]

Component licensing status
==========================
Device control:           Licensed
Application control:      Licensed
Application behavior:     Licensed
Security awareness:       Licensed
Encryption 2-Go:          Licensed
File Protection:          Licensed
BitLocker management:     Licensed
BitLocker PBA option:     Licensed
BitLocker To Go:          No
Disk Protection:          No
Legacy OS option:         No
Vulnerability scan:       Licensed
                          With standard vulnerability catalog
Windows Defender:         Licensed
Native Security:          No
EDR:                      Licensed

Current agent status
====================
Environment:            Production
FDE special config:     No
Appl. terminal srv.:    No
Reboot pending:         No
Temporary unlock:       Not active
Policy config source:   Not available (NoStore)
Local config source:    C:\ProgramData\CenterTools DriveLock\Conf:
Configuration type:     CSP assignments

Current Application Control Status
==================================
Blocking mode:          Whitelist, including DLLs (simulate)
Local Whitelist:        Present

Current Microsoft Defender Control status
=========================================
Defender Control is active

Agent configuration
===================
```

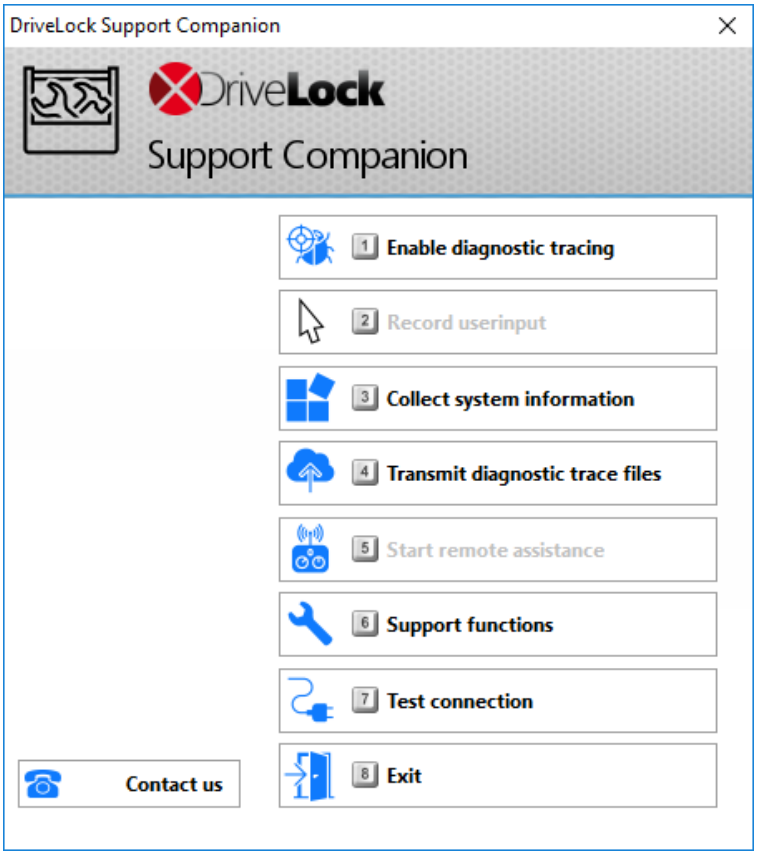
OK

Sie können diesen Text markieren und per Copy & Paste weiterverwenden.

6.2 DriveLock Support Companion

Die einfachste Methode eine Trace-Datei zu erstellen, ist direkt am Client durch Aufruf einer der folgenden Dateien

- Dlsupport.exe: Wird mit der MMC installiert. Enthält den Teamviewer als Fernwartungsprogramm.
- Dlsupportagent.exe: Wird mit dem DriveLock Agenten installiert. Enthält kein Fernwartungsprogramm. Im Regelfall verwenden Sie diese Datei.



Wenn Sie die Option **Test connection** wählen, können Sie die Verbindung vom DriveLock Agenten zum DriveLock Enterprise Service (DES) überprüfen. Der DriveLock Connectivity Analyzer analysiert die Verbindung und erstellt eine Auflistung aller wichtigen Verbindungsparameter (Connectivity Report), beispielsweise die TCP- und MQTT-Verbindungen, Fernkontrolleinstellungen des Agenten oder die Überprüfung der Zertifikate. Des weiteren wird die korrekte Registrierung und Identität des Agenten am DES überprüft, sofern der Agent mit einem Beitrittstoken aus dem DOC heraus neu installiert wurde.

7 Terminalserver

DriveLock unterstützt die Verwendung auf Terminalservern. Die Module Device Control und Application Control 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.

7.1 Verbindungsarten

Unterstützte Funktionen je nach Verbindungsart (nur Laufwerksverbindungen):

Funktion	FAT Clients	Windows Embedded Client	Virtual Clients	Thin Clients
Berechtigungen anhand von Benutzer / Gruppen	Ja	Ja	Ja	Ja
Freigabe anhand des verbundenen Laufwerksbuchstaben	Ja	Ja	Ja	Ja
Freigaben anhand der Hardwaredaten inkl. Seriennummer	Ja	Ja	Ja	Nein
Dateisystemfilter	Ja	Ja	Ja	Ja
Dateisystemfilter inkl. Header Überprüfung	Ja	Ja	Ja	Ja
Dateiprotokollierung	Ja	Ja	Ja	Ja

Funktion	FAT Clients	Windows Embedded Client	Virtual Clients	Thin Clients
Schattenkopie	Ja	Ja	Ja	Ja
Benötigt DriveLock-Agent lokal	Ja	Ja	Ja	Nein
Benötigt DriveLock-Agent auf dem TS	Nein	Nein	Der Virtual-Client wird anstatt des Terminalservers verwendet.	Ja

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

FAT-Clients / Desktop-Clients

Ein FAT-Client bzw. ein Desktop-Client ist ein normaler Computer mit Windows. 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.

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.

Virtual Desktop Infrastructure (VDI)

Ein Virtual-Client ist ein virtueller Computer mit Windows. Ein Client stellt eine Verbindung mit dem virtuellen Desktop 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.

Thin-Clients

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.

Copyright