DriveLock Installation

Dokumentation 2022.2

DriveLock SE 2022

Inhaltsverzeichnis

1 Willkommen zur Installation von DriveLock

DriveLock hat es sich zum Ziel gesetzt, Daten, Geräte und Systeme von Unternehmen zu schützen. Hierfür setzt DriveLock auf neueste Technologien, erfahrene Security-Experten und Lösungen nach dem Zero Trust Modell.

Dieses Installationshandbuch unterstützt Sie bei der ersten Installation von DriveLock und liefert Ihnen Anleitungen, wie Sie schnell und einfach die Management-Komponenten von DriveLock auf Ihrem Server und den DriveLock Agenten auf den Client-Computern in Ihrem Netzwerk installieren können.

Als Alternative zur Installation und selbständigen Einrichtung Ihrer Umgebung bietet Ihnen DriveLock aber auch eine umfassende Sicherheitslösung durch unseren Cloud-basierten Managed Security Service an. Dieser beinhaltet u.a. Hosting der kompletten Lösung, Verwaltung durch Sicherheitsexperten und Zuschneiden von Sicherheitsstandards auf individuelle Anforderungen.

> Hinweis: Beachten Sie bitte, dass es für Managed Security Service eine eigenständige Dokumentation gibt, die Ihnen als Managed-Service-Benutzer automatisch zur Verfügung gestellt wird.

2 Vor der Installation des DriveLock Enterprise Service (DES)

Wir empfehlen folgende Vorbereitungen, bevor Sie mit der Installation von DriveLock beginnen.

Notwendige Vorbereitungen:

- Legen Sie ein Konto an, unter dem der DriveLock Enterprise Service (DES) laufen soll. Dieses Konto muss nicht über Administratorrechte verfügen.
- Für die Installation des DES benötigen Sie mindesten einen Windows Server 2012 R2
- Der DES benötigt den Microsoft SQL Server 2012 Native Client Version 11.4.7001.0. Wenn diese Komponente nicht installiert ist, geschieht dies automatisch vor der eigentlichen Installation des DES. Wenn eine ältere Version installiert ist, wird diese automatisch aktualisiert.

Optionale Vorbereitungen:

1. Wenn Sie eine eigene Zertifizierungsstelle haben, legen Sie ein Server-Zertifikat für die Client-Server-Authentifizierung an.
   Anforderungen an das SSL-Zertifikat, das für den DES verwendet werden soll:
   - Signaturalgorithmus: sha256SA
   - Länge des öffentlichen Schlüssels: RSA 2048/4096 Bit
   - Erweiterte Verwendung:
     - Server-Authentifizierung (1.3.6.1.5.5.7.3.1)
     - Client-Authentifizierung (1.3.6.1.5.5.7.3.2)
   - Verwendung des Schlüssels: Digitale Signatur, Schlüsselverschlüsselung
   - Beim Import in den Zertifikatsspeicher muss unbedingt die Option **Privaten Schlüssel des Zertifikats als exportierbar markieren** gesetzt sein.
   - Das Zertifikat muss einen Anzeigenamen (Friendly Name) haben
   - DNS-Alias: Wenn ein DNS-Alias für den DES-Server verwendet wird, muss das Zertifikat auch für diesen DNS-Alias ausgestellt werden
   - Das Zertifikat muss vor der Installation von DriveLock im Speicher "Lokaler Computer - Eigene Zertifikate" installiert werden
     Weitere Informationen zu Zertifikaten finden Sie im Kapitel Vertrauenswürdige Zertifikate in der Dokumentation DriveLock Administration auf DriveLock Online

Help.

> Achtung: DriveLock unterstützt keine Wildcard-Zertifikate für den DES.

2. Wenn Sie nicht den mitgelieferten Microsoft SQL Express Server verwenden wollen (für kleine Umgebungen und Testumgebungen), benötigen Sie einen Microsoft SQL Server.
3. Wenn der Benutzer, der den DES installiert, nicht die nötigen Berechtigungen auf dem Datenbankserver hat, sollte der Datenbank-Administrator folgende Vorbereitungen treffen:
   - Anlegen einer Microsoft SQL Server Datenbank für DriveLock
   - Der Login, der bei der Installation verwendet wird, benötigt nur die SQL Server Rolle **public** und muss Mitglied der **db_owner** Rolle in der DriveLock Datenbank sein.
4. Wenn mehrere Benutzer für die Administration von DriveLock zuständig sein sollen, ist es sinnvoll, eine AD-Gruppe für die Benutzer anzulegen, die administrative Berechtigungen für DriveLock haben soll.

> Hinweis: Weitere Informationen zu diesen Themen finden in Sie den aktuellen Release Notes oder in der Dokumentation DriveLock Administration auf DriveLock Online Help.

3 Installation der DriveLock-Komponenten

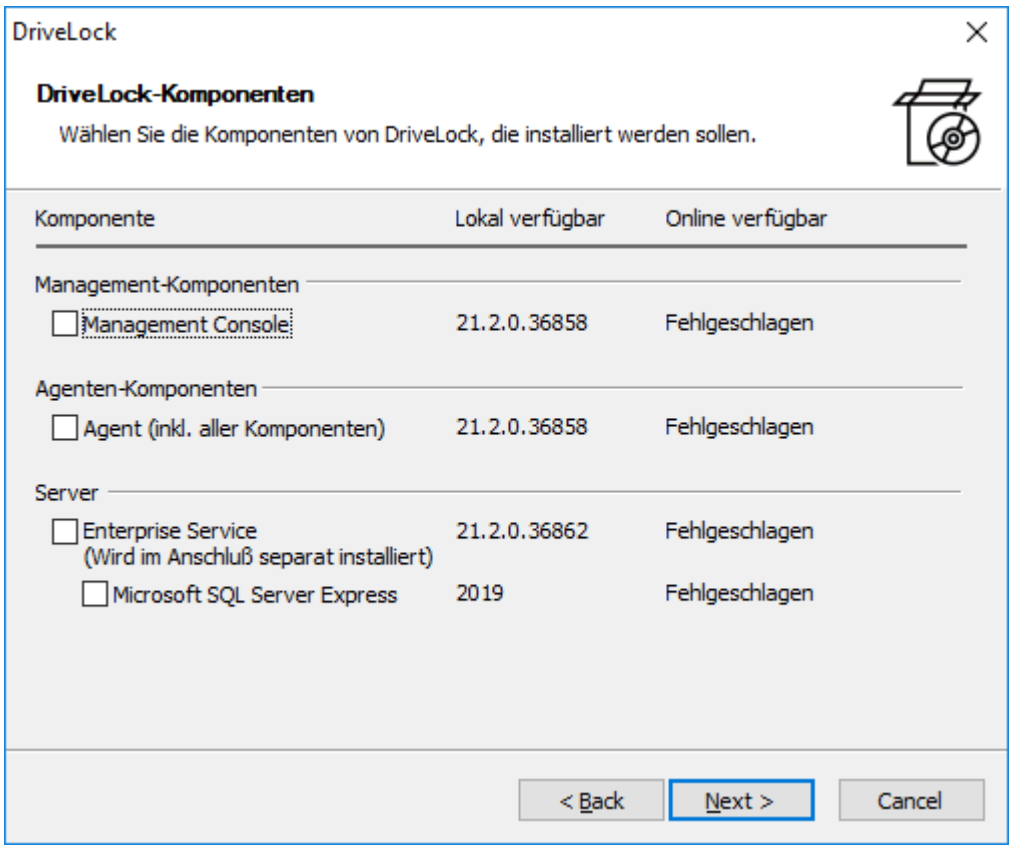
Wir empfehlen, die Management-Komponenten auf dem Server mitzuinstallieren.

Sie können die Management-Komponenten aber auch auf einzelnen Client-Computern separat installieren, wenn beispielsweise verschiedene Mitarbeiter auf diesen Computern mit den Management-Komponenten arbeiten sollen.

3.1 Auswahl der Komponenten

Der Installationsassistent unterstützt Sie bei der Installation. Gehen Sie dabei folgendermaßen vor:

1. Führen Sie über das ISO-Image die Datei **DLSetup.exe** aus
2. Wählen Sie Ihre Sprache und akzeptieren Sie die DriveLock EULA.
3. Wählen Sie folgende Komponenten, wie in der Abbildung gezeigt:
    - DriveLock Management Konsole
    - Enterprise Service
      Optional können Sie einen Microsoft MS SQL Express Server als Datenbankserver mitinstallieren.
      Ab 200 Geräten (Enterprise-Umgebung) wird ein vollwertiger SQL Server empfohlen.



Hinweis: Die Option **Agenten-Komponenten** benötigen Sie nur im Falle einer Testinstallation.

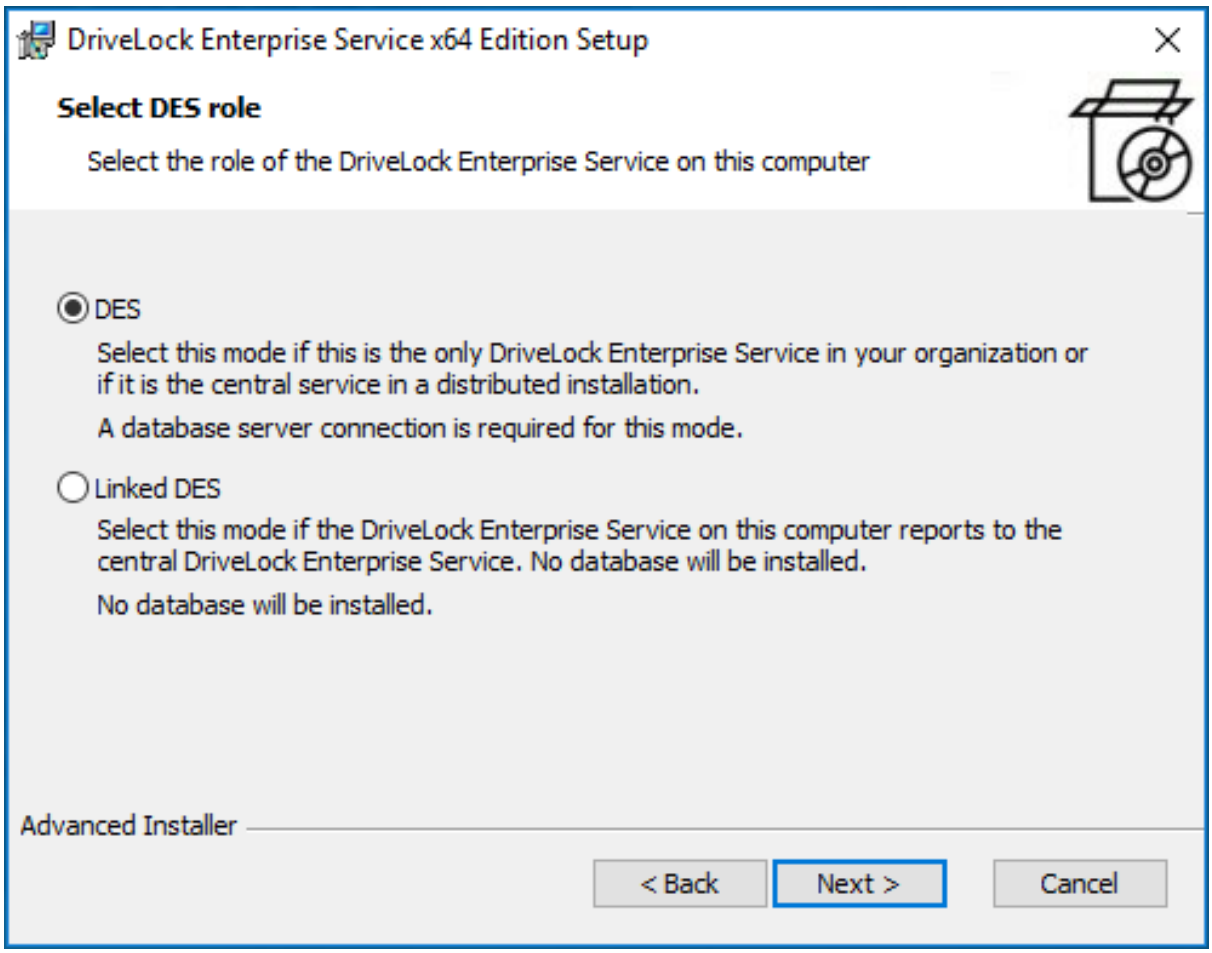
4. Im nächsten Dialog werden Ihnen die gewählten Komponenten angezeigt. Folgende Optionen sind verfügbar:
   - Die Option **Keine aktualisierten Versionen herunterladen – vorhandene Dateien benutzen** ermöglicht Ihnen die Installation der im aktuellen Verzeichnis gespeicherten Versionen.
   - Sie können die Option **Dateien nur herunterladen – nicht installieren** wählen, wenn Sie die zuvor ausgewählte Komponenten nicht sofort installieren sondern nur über das Internet laden wollen.
5. Klicken Sie nun auf **Weiter**, um mit dem Download bzw. der Installation zu beginnen. Im letzten Dialog erhalten Sie eine Auflistung der erfolgreich installierten Komponenten.
6. Als nächstes öffnet sich der Assistent zur Installation des DriveLock Enterprise Service. Dieser wird nur in englischer Sprache angeboten.

3.2 Installation des Servers

Gehen Sie folgendermaßen vor:

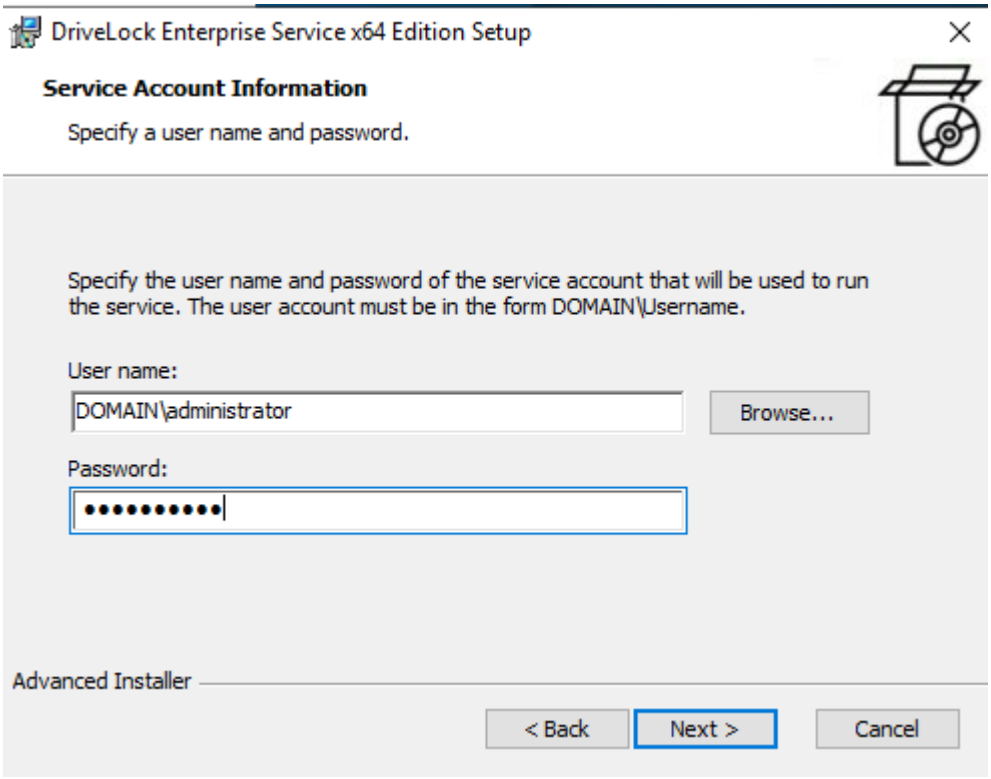
1. Klicken Sie im Begrüßungsdialog auf **Next** und bestätigen Sie dann im folgenden Dialog die Endbenutzer-Lizenzvereinbarung (EULA).
2. Geben Sie nun an, welche Rolle Ihr neuer DriveLock Enterprise Service (DES) einnehmen wird. Wählen Sie hier die Option **DES**.

   Hinweis: Der erste DES, den Sie anlegen, muss immer ein zentraler DES sein.

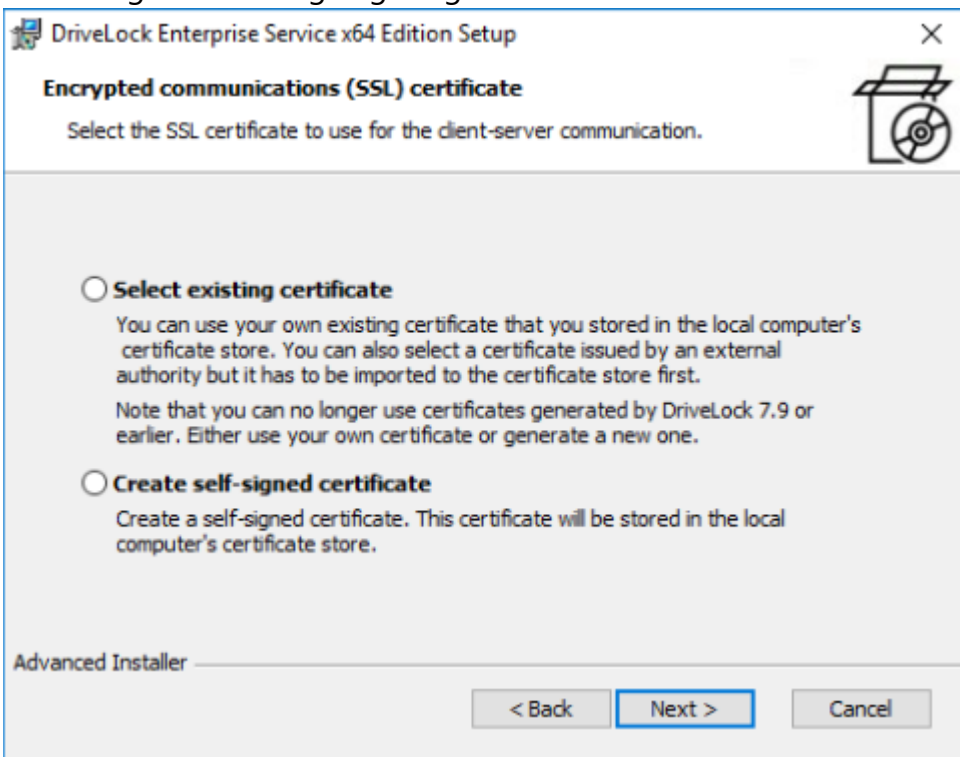


   Die Option **Linked DES** können Sie dann auswählen, wenn Ihre Infrastruktur mit zentralem DES bereits eingerichtet ist, und Sie verknüpfte DES hinzufügen wollen. In diesem Fall muss dann keine Datenbank mehr erstellt werden.

3. Im nächsten Dialog geben Sie das Dienstkonto und das dazugehörige Kennwort ein, unter welchem der DriveLock Enterprise Service gestartet werden soll.
   Klicken Sie auf **Browse...**, um ein bestehendes Konto auszuwählen.



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



Hier haben Sie zwei Möglichkeiten:

- Wählen Sie **Select existing certificate**, wenn Sie über ein eigenes Zertifikat im Zertifikatsspeicher des Computers verfügen und dieses verwenden wollen.

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

- Wählen Sie **Create self-signed certificate**, wenn DriveLock ein SSL-Zertifikat für Sie erstellen soll. Wenn Sie DriveLock in Testumgebungen verwenden, kann diese Option empfehlenswert sein.
  Weitere Informationen zu Zertifikaten finden Sie hier.

5. Klicken Sie im nächsten Dialog auf die Schaltfläche **Install**, um die Installation des DES fortzusetzen.
6. Nach Beendigung der Installation klicken Sie **Finish**, um die Installation abzuschließen. Anschließend startet automatisch der Assistent für die Datenbank-Installation.

3.3 Installation der Datenbank

DriveLock unterstützt als Datenbanksystem Microsoft SQL Server und Microsoft SQL Server Express. Die genauen Spezifikationen entnehmen Sie bitte den aktuellen Release Notes auf DriveLock Online Help.

3.3.1 Unterschiedliche Vorgehensweisen nach Umgebungstyp

Übersicht über die unterschiedlichen Szenarien bei der Datenbankinstallation:

	Szenario 1: kleine Umgebungen	Szenario 2: große Umgebungen	Szenario 3: Enterprise-Umgebungen
Datenbankserver	SQL Express	Microsoft SQL Server	Microsoft SQL Server
Manuelles Anlegen der Datenbank	nein	nein	ja
Erforderliche Berechtigungen	SQL Express und DES werden im Zuge des DriveLock Setups (DLSetup.exe) installiert. Hierbei wird das Benutzerkonto, das die Installation durch-	Login auf SQL Server mit den Rollen **dbcreator** und **securityadmin**	Der Login, der bei der Installation verwendet wird, benötigt in diesem Fall dann nur die SQL Server Rolle **public** und muss Mitglied der **db_**

	führt, zum Administrator der SQL Express Datenbank		**owner** Rolle in der DriveLock Datenbank sein.
Erforderliche Optionen für die Datenbank-Installation:			
Datenbank erstellen	ja	ja	nein
Datenbanklogin erstellen	ja	ja	nein
DES-Dienstkonto zum Eigentümer der Datenbank machen	ja	nein	nein
Datenbankwartung, Datenbereinigung und Backups	via DES	via SQL Server aufsetzen	via SQL Server aufsetzen

Hinweis: Weitere Informationen finden Sie hier und im DriveLock Database Guide (nur verfügbar auf Englisch) unter Technical Articles auf DriveLock Online Help.

3.3.2 Datenbank-Installationsassistent

Gehen Sie folgendermaßen vor, um die Datenbank zu installieren:

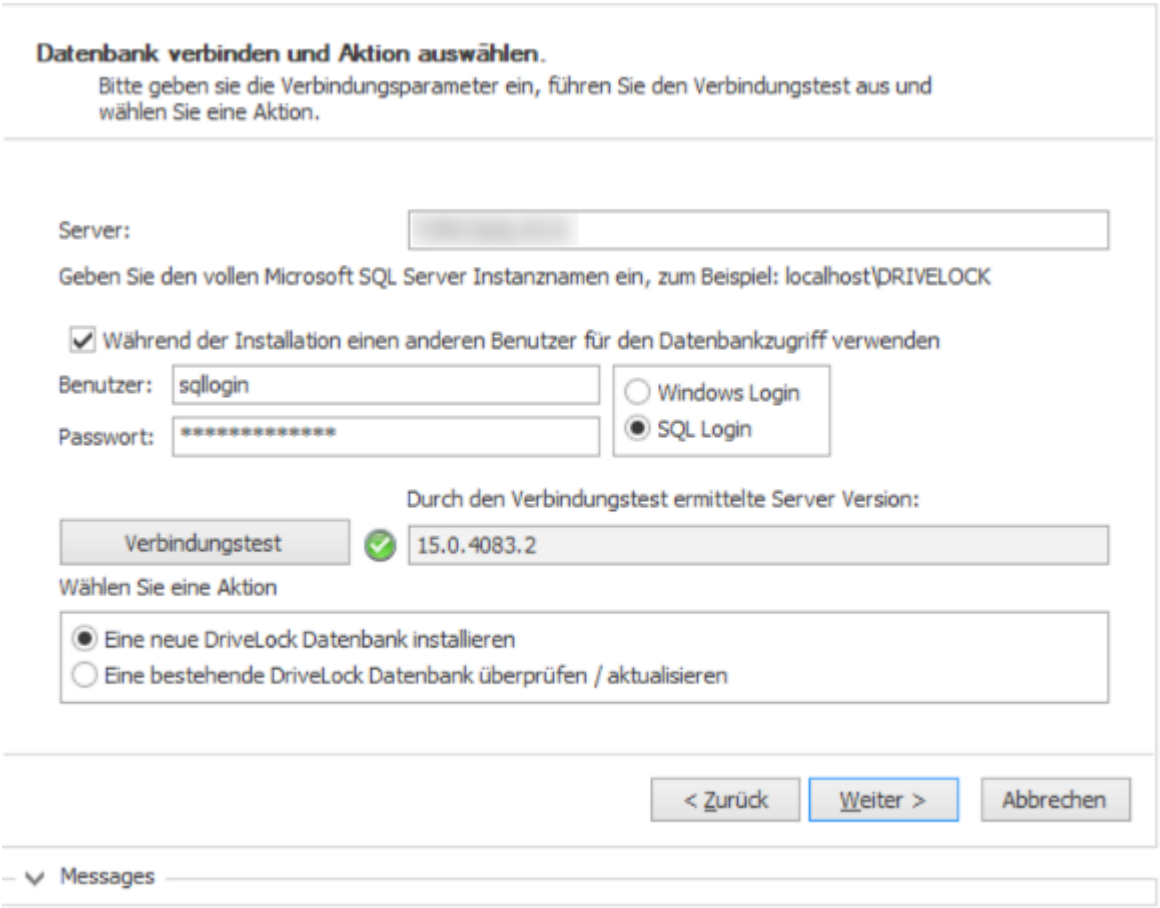
1. Klicken Sie im Begrüßungsdialog **Willkommen zum DriveLock Datenbank-Installationsassistent** auf **Weiter**.
2. Wählen Sie im folgenden Dialog die Option **Zentraler DriveLock Enterprise Service**, wenn Sie eine neue Datenbank erstellen wollen.
   Diese Option ist standardmäßig ausgewählt, wenn Sie bei der Installation des Servers die Option DES gewählt haben.

- Die Option **Verknüpfter DriveLock Enterprise Service** eignet sich zum Anlegen von verknüpften DES, wofür Sie keine erneute Datenbankinstallation durchführen müssen.
- Die Option **Verknüpfter DriveLock Enterprise Service zur Anbindung an die Cloud** wird verwendet, wenn Sie die DriveLock Managed-Service-Lösung verwenden und Agenten haben, die über keine direkte Internetverbindung verfügen. In diesem Fall kann die Verbindung zur DriveLock Cloud über den verknüpften DES als Vermittler hergestellt werden. Weitere Informationen zu verknüpften DES finden Sie im Administrationshandbuch auf DriveLock Online Help.

3. Geben Sie als nächstes die Verbindungsdaten für den Datenbankserver an.
   - Hier kann optional ein anderer Benutzer für den Datenbankzugriff angegeben werden. Windows- und SQL Server-Authentifizierung sind möglich. Diese Daten werden nicht gespeichert und ausschließlich für die Installation/Update verwendet.

> Hinweis: Sollten Sie den Port mitangeben wollen, unterstützt der Datenbank-Installationsassistent folgende Schreibweise: FQDN,Port\Instanz (z.B.: myDLServer,14330\SQLEXPRESS)

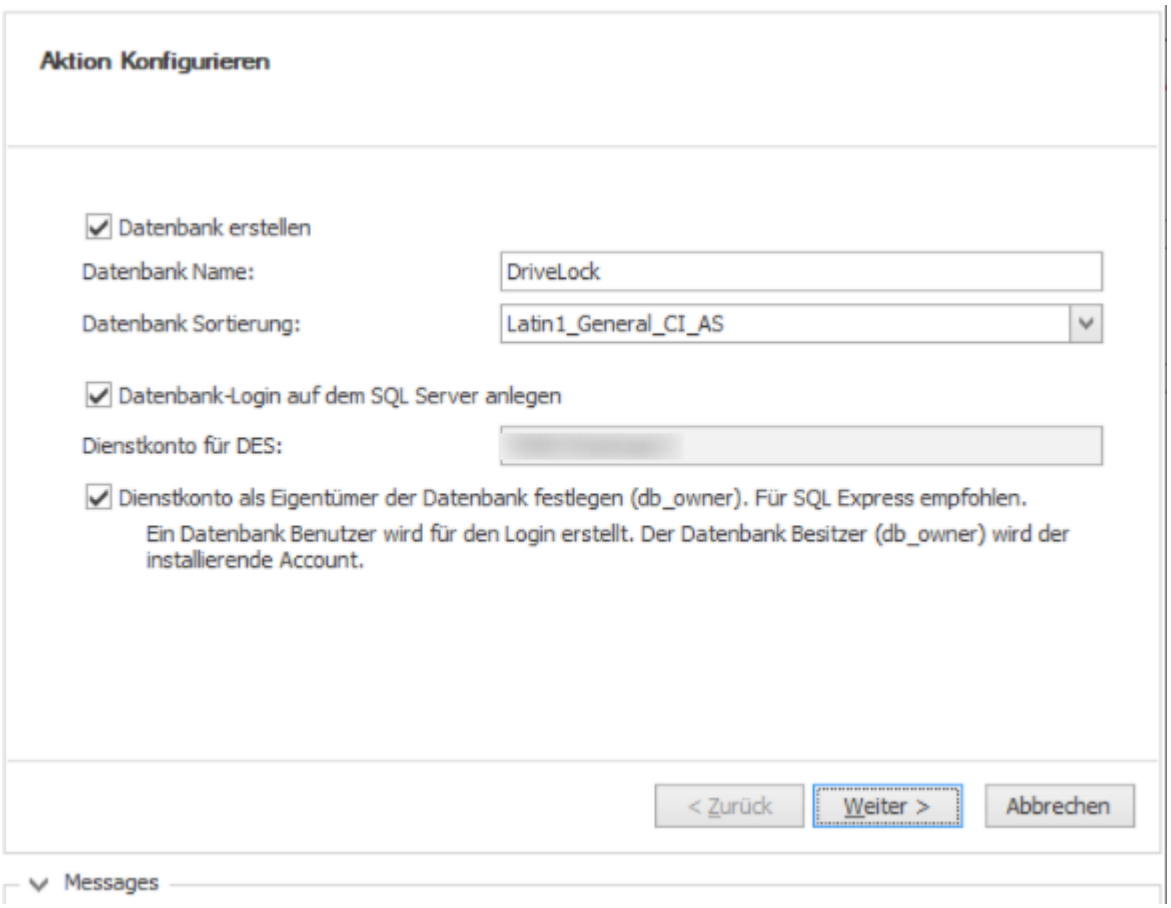
- Nach Eingabe des Servernamens klicken Sie die Schaltfläche **Verbindungstest**. Wenn ein grünes Häkchen erscheint, ist die Verbindung zustande gekommen. Sollte es zu Verbindungsproblemen kommen, werden Ihnen diese im Bereich unter **Messages** angezeigt. Sie können dann eine entsprechende Lösung finden.
- Wählen Sie als Aktion **Eine neue Datenbank installieren**.



4. Bei der Erstellung der Datenbank gibt es mehrere Möglichkeiten, die sich nach bestimmten Szenarien richten.
   - **Datenbank erstellen**:
     Diese Option ist standardmäßig gesetzt. Die Datenbank wird auf dem SQL Server erstellt. Das Konto, das die Installation durchführt, muss entsprechende Berechtigungen auf dem SQL Server haben (dbcreator Rolle). Wenn Sie diese Option abwählen, müssen Sie eine Datenbank bereitstellen. Das Schema wird dann in diese Datenbank installiert.
   - **Datenbank-Login auf dem SQL Server anlegen**:
     Diese Option ist auch standardmäßig gesetzt. Ein Login wird für das **Dienstkonto des DES** erstellt. Das Konto, das die Installation durchführt, muss

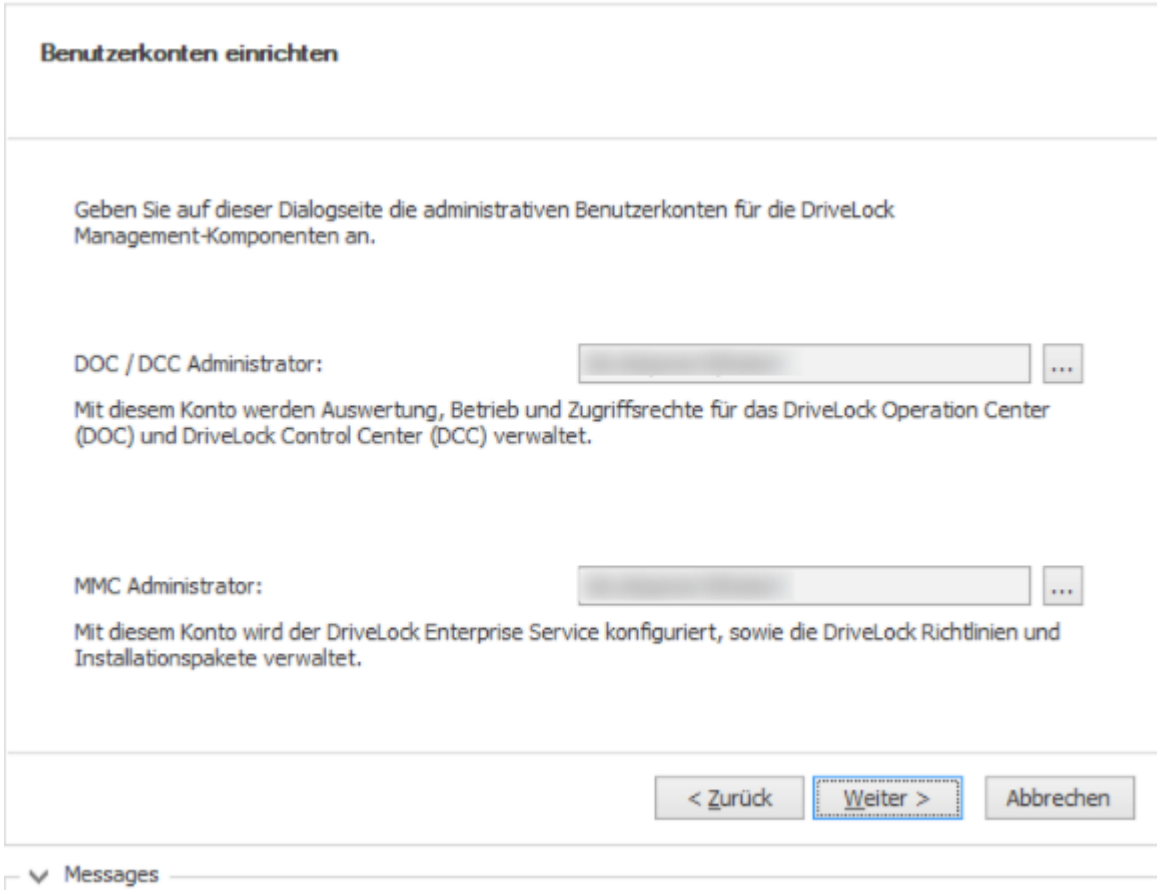
entsprechende Berechtigungen auf dem SQL Server haben (securityadmin Rolle).

- **Dienstkonto als Eigentümer der Datenbank festlegen (db_owner). Für SQL Express empfohlen**:
  Diese Option ist nicht standardmäßig gesetzt. Durch sie erhält das DES-Dienstkonto maximale Rechte auf die DriveLock Datenbanken und kann dadurch Aufgaben wie beispielsweise Wartung (Indexpflege), Bereinigung von alten Datensätzen und Backup der Datenbank übernehmen.
  Für größere Umgebungen bzw. beim Betrieb auf einem vollen SQL Server empfehlen wir, diese Option auszuschalten.



5. Als nächstes geben Sie die Benutzerkonten für das DOC bzw. DCC und die Management Konsole an. In der Regel ist dies der Benutzer, unter dem die Installation durchgeführt wird.
   - **DOC / DCC Administrator**: dieser Benutzer oder diese Gruppe darf später auf das DriveLock Operations Center und das DCC zugreifen (Vollzugriff). Weitere Berechtigungen können später angepasst werden.

- **MMC Administrator**: dieser Benutzer oder diese Gruppe darf später innerhalb der DriveLock Management Konsole DriveLock Enterprise Service Einstellungen konfigurieren. Weitere Berechtigungen können später in der DriveLock Management Konsole vergeben werden



6. Aktionen ausführen: Die Datenbankinstallation wird durchgeführt. Klicken Sie auf **Weiter**.
7. Im nächsten Dialog geben Sie an, ob Sie die Datenbankwartung bzw. -sicherung aktivieren möchten. Übernehmen Sie die Standardoptionen.
   Wenn Sie die Einstellungen zu einem späteren Zeitpunkt ändern wollen, können Sie dies in den DES-Eigenschaften tun. Weitere Informationen finden Sie im Kapitel Wartung und Bereinigung des Administrationshandbuchs auf DriveLock Online Help.
8. Als letztes wird Ihnen eine Zusammenfassung angezeigt. Klicken Sie zum Abschluss auf **Fertigstellen**.

4 Initiale Konfiguration in der DriveLock Management Konsole

Sobald Sie die Installation der DriveLock Komponenten, des DES und der Datenbank abgeschlossen haben, erscheint in Ihrem Startmenü ein neuer Eintrag **DriveLock**. Starten Sie hier die **DriveLock Management Console**.

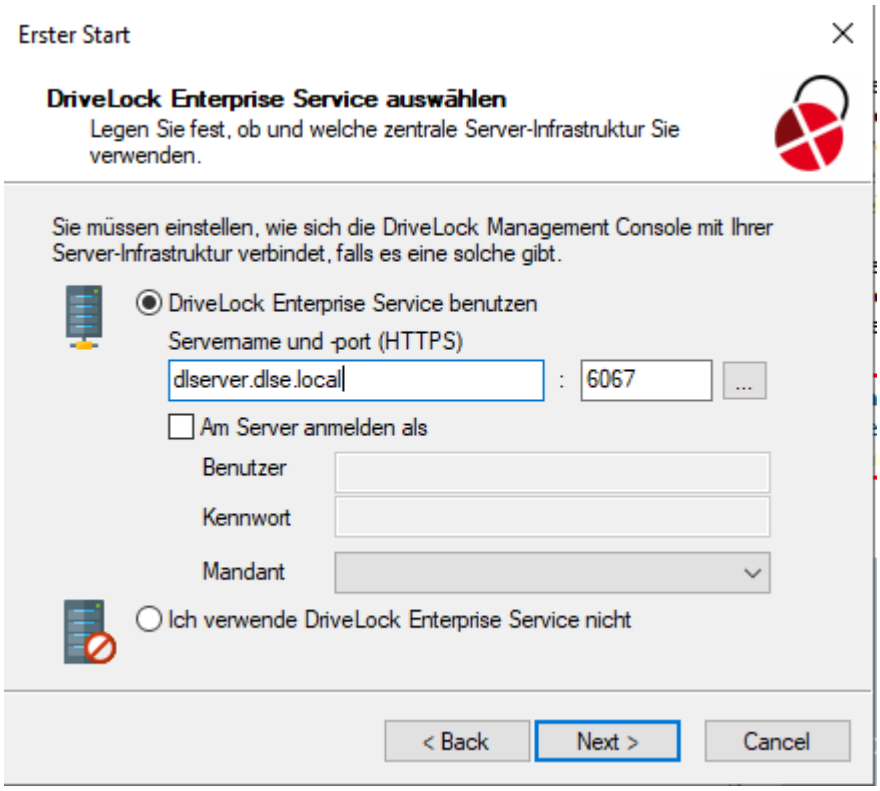
Tipp: Heften Sie diesen Eintrag an Ihre Taskleiste an.

4.1 Erste Konfigurationsschritte

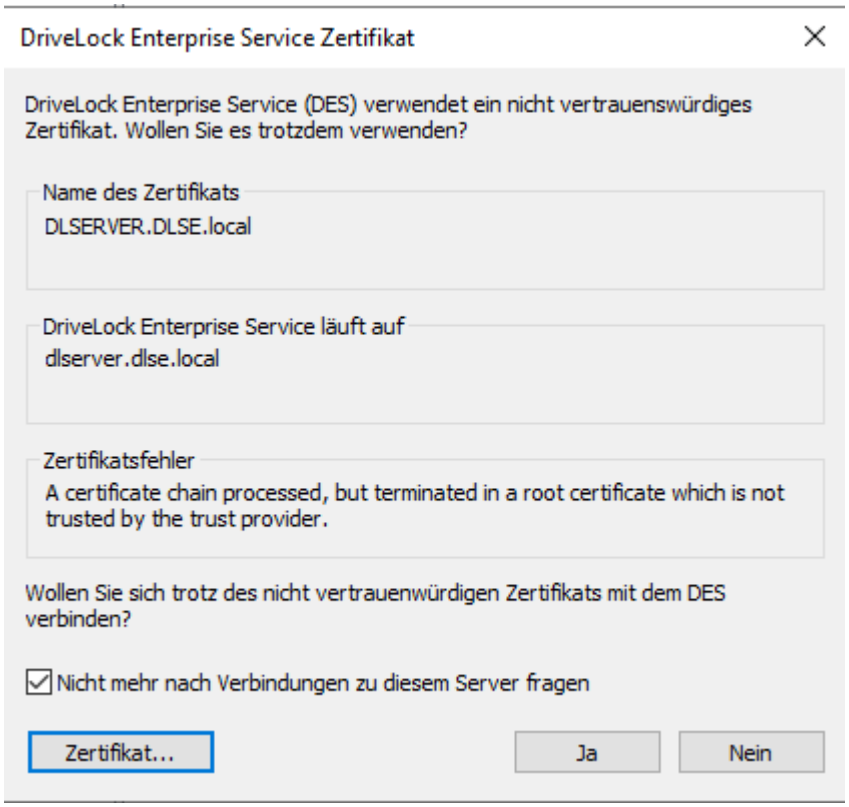
Als erstes startet ein Assistent, der Sie beim Einrichten der Verbindungseinstellungen zum DriveLock Enterprise Service (DES) unterstützt.

Gehen Sie folgendermaßen vor:

1. Nach Bestätigen des Begrüßungsdialogs wählen Sie im nächsten Dialog die Option **DriveLock Enterprise Service benutzen** aus.
   - Geben Sie den Servernamen und den Port ein. Verwenden Sie hierbei einen vollqualifizierten Namen. Als Port verwenden Sie 6067. Weitere Informationen zu den Ports finden Sie hier.
   - Wählen Sie den Standardmandanten **root** aus der Dropdown-Liste unter **Mandant** aus.
   - Wenn Sie für Ihren Server einen anderen Benutzer angeben wollen, geben Sie die entsprechende Information an. Dies kann beispielsweise zur Einschränkung von Rechten sinnvoll sein.



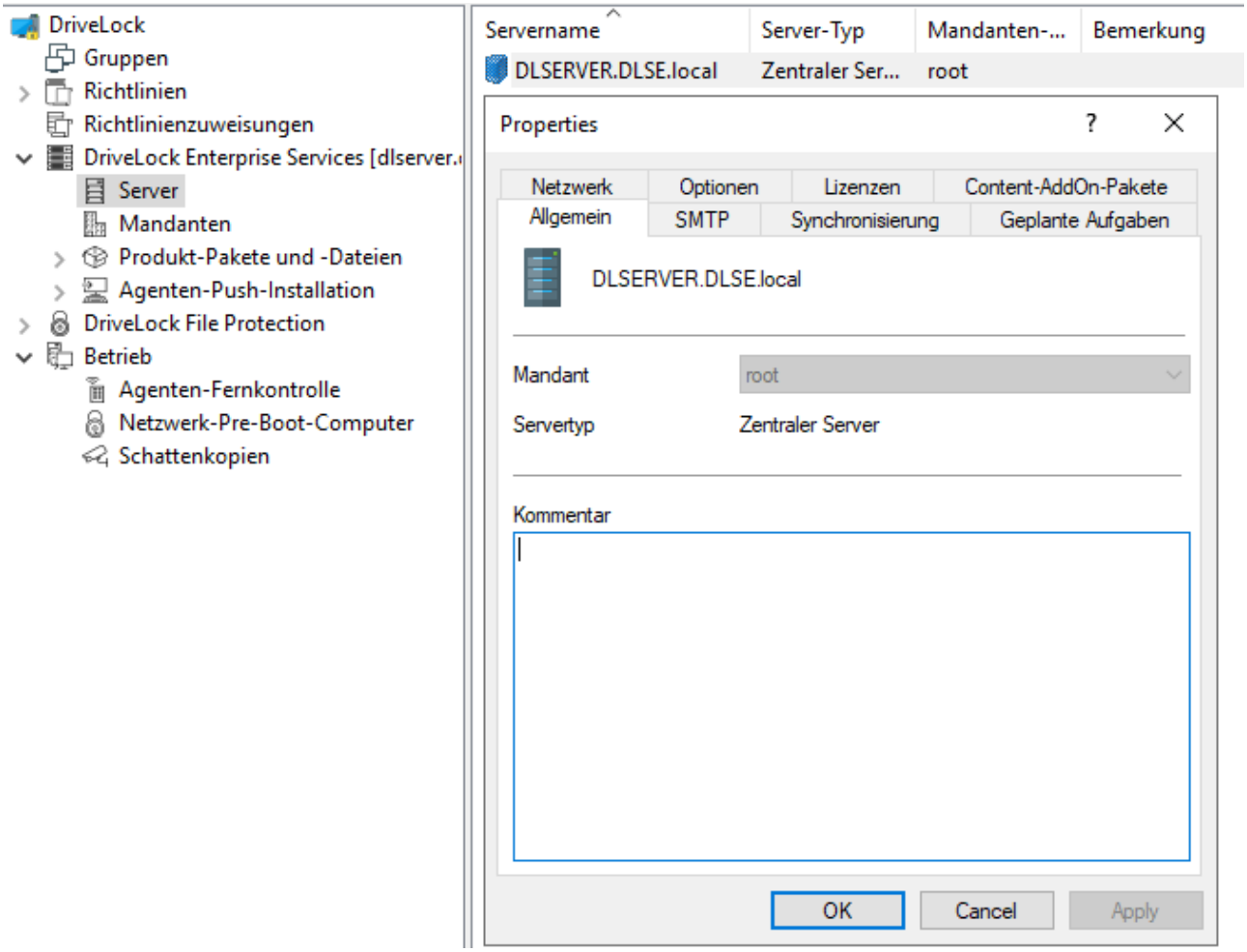
2. Wenn der DES ein selbstsigniertes Zertifikat verwendet, müssen Sie anschließend das Zertifikat als vertrauenswürdig bestätigen.
   - Klicken Sie auf die Schaltfläche **Zertifikat...**, um zu prüfen, dass es sich tatsächlich um das Zertifikat handelt, das der DES verwendet.
   - Setzen Sie ein Häkchen bei der Option **Nicht mehr nach Verbindungen zu diesem Server fragen**.
   - Bestätigen Sie den Dialog mit **Ja**, um das Zertifikat zu verwenden.
     Weitere Informationen zu Zertifikaten finden Sie hier.



3. Im abschließenden Dialog geben Sie an, wie oft geprüft werden soll, ob neue Versionen der DriveLock Management Konsole zur Verfügung stehen. Der Versionsstatus wird direkt über die DriveLock Cloud abgefragt.
4. Klicken Sie auf **Fertigstellen**, um Ihre Angaben zu bestätigen.

4.2 Erste Einstellungen am DES

Sobald Sie die initialen Konfigurationsschritte abgeschlossen haben, ist Ihr zentraler Server im Knoten **DriveLock Enterprise Services** eingetragen.



Im Eigenschaftendialog nehmen Sie zunächst folgende Einstellungen vor:

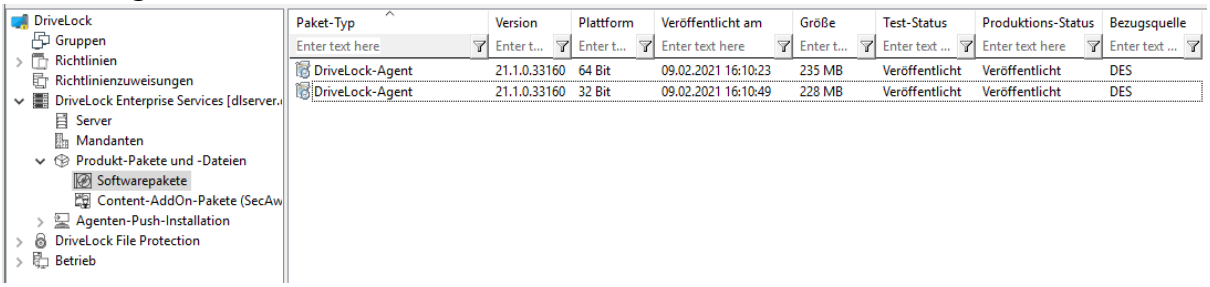
1. Auf dem Reiter **Netzwerk** ist die Einstellung **HTTPS erzwingen** standardmäßig gesetzt. Mit dieser Option wird sichergestellt, dass die Kommunikation nur noch über HTTPS und nicht über HTTP stattfindet. Weitere Informationen finden Sie hier. Auf diesem Reiter können Sie auch die Einstellungen für Proxyserver angeben.
2. Lassen Sie auf dem Reiter **Synchronisierung** die Option **Softwareaktualisierungen aus dem Internet herunterladen** aktiviert, so dass die Softwarepakete für Ihre DriveLock-Komponenten immer auf dem aktuellen Stand sind.
3. Sobald Sie Ihre Einstellungen abgeschlossen haben, werden Sie aufgefordert, den DES neu zu starten.

4.3 Erstes Hochladen der Agenten-Pakete auf den DES

Wir empfehlen die Agenten-Pakete auf den DES hochzuladen und zu veröffentlichen, damit Auto-Update und Push-Installation funktionieren.

Gehen Sie folgendermaßen vor:

1. Auf dem DriveLock ISO-Image befinden sich die beiden msi-Pakete für den DriveLock Agenten. Kopieren Sie sie an beliebige Stelle auf Ihrem Computer.
2. Gehen Sie dann in der DriveLock Management Konsole zum Knoten **Produkt-Pakete und -Dateien** , markieren **Softwarepakete** und wählen aus dem Kontextmenü **Paket hochladen**.
3. Wählen Sie das entsprechende Paket (bzw. die beiden Agenten-Pakete) aus und laden Sie sie zum DES hoch. Sie erscheinen dann in der Liste der Softwarepakete.
4. Veröffentlichen Sie nun die Pakete in der Test- und/oder Produktionsumgebung, s. Abbildung:



Weitere Informationen zur Push-Installation finden Sie im entsprechenden Kapitel im Administrationshandbuch auf DriveLock Online Help.

4.4 Erste Schritte bei der Erstellung von Richtlinien

In einer DriveLock-Richtlinie werden alle Einstellungen gespeichert, die der DriveLock Agent benötigt. Jedes DriveLock Modul (wie z. B. Device oder Application Control oder Verschlüsselung) hat einen eigenen Bereich innerhalb der Richtlinie, in dem alle Einstellungen dieses Moduls gespeichert sind.

Das Arbeiten mit zentral gespeicherten Richtlinien hat sich bei DriveLock u.a. aus folgenden Gründen bewährt:

- Sie werden in der DriveLock-Datenbank gespeichert und dann von den Agenten von dort über den DriveLock Enterprise Service bezogen.
- Zudem unterliegen zentral gespeicherte Richtlinien automatisch einer Versionierung und können vom Administrator separat bearbeitet oder veröffentlicht werden.
- Sie können eine beliebige Anzahl von Richtlinien erstellen und Agenten zuweisen oder auch nur eine einzige. Beachten Sie hier auch den Hinweis unter Lizenzen.

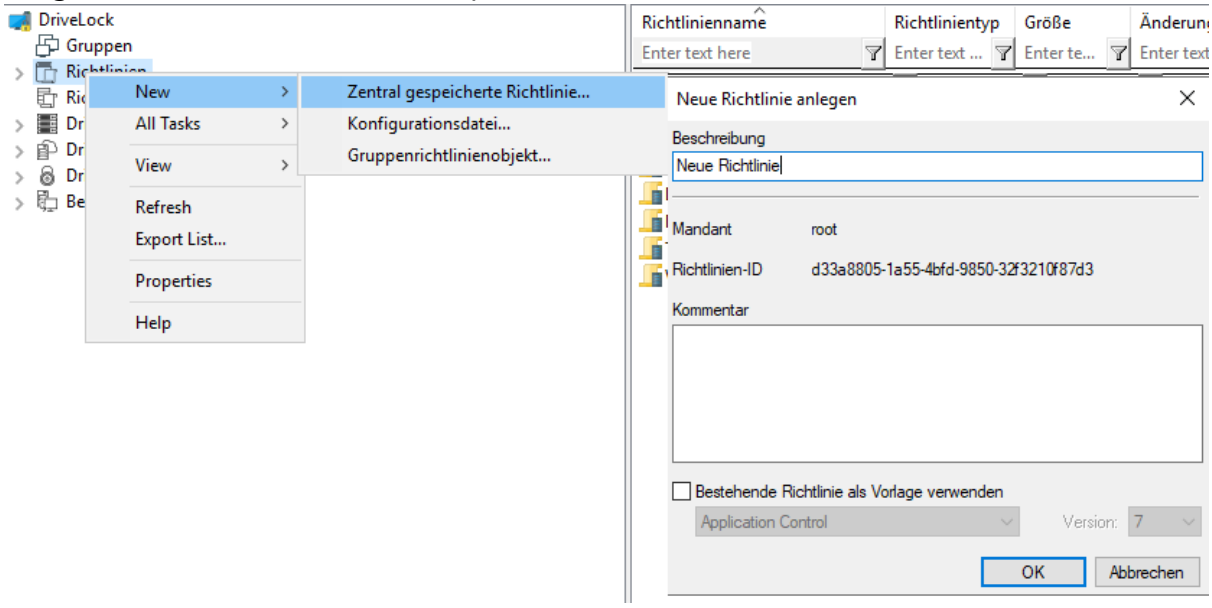
Eine ausführliche Beschreibung sämtlicher Funktionen finden Sie im Administrationshandbuch auf DriveLock Online Help.

Im Folgenden erstellen Sie Ihre erste zentral gespeicherte Richtlinie, nehmen einige Grundeinstellungen vor und weisen die Richtlinie dann zu.

4.4.1 Erste zentral gespeicherte Richtlinie erstellen

Gehen Sie folgendermaßen vor:

1. Öffnen Sie im Knoten Richtlinien das Kontextmenü, wählen Sie **Neu** und dann **Zentral gespeicherte Richtlinie...**.
2. Vergeben Sie einen Namen und speichern Sie die neue Richtlinie.



3. Die neue Richtlinie erscheint jetzt in der Liste.
4. Wählen dann als erstes den Knoten **Globale Einstellungen**. Die im Folgenden beschriebenen Einstellungen sind Grundeinstellungen und sorgen für eine Minimalkonfiguration. Alle anderen Einstellungen sind im Administationshandbuch erläutert.

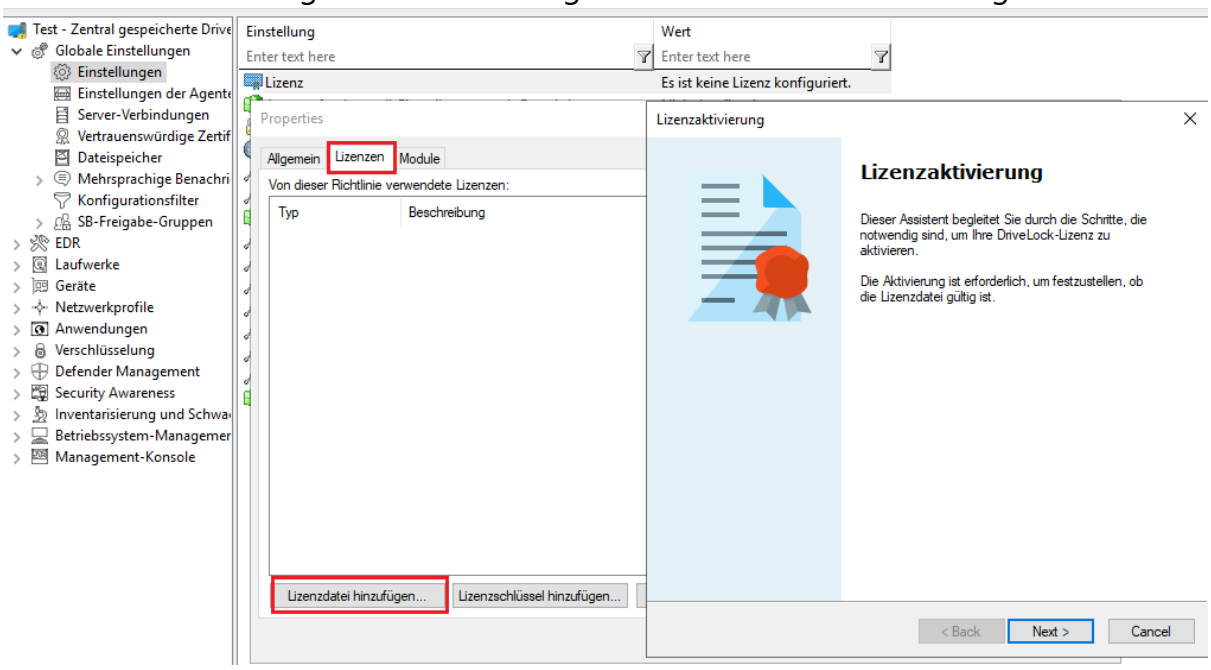
4.4.1.1 Lizenzen

Tragen Sie zunächst Ihre DriveLock Lizenzen direkt in der Richtlinie ein.

> Hinweis: Wenn Sie eine einzige Richtlinie für alle Ihre Einstellungen verwenden wollen, können Sie in dieser die Lizenzeinstellungen direkt setzen. Wenn Sie allerdings verschiedene Richtlinien verwenden, empfehlen wir die Erstellung einer separaten Lizenz-Richtlinie, die nur die Lizenzeinstellungen enthält und dann den Agenten zugewiesen wird.

Gehen Sie folgendermaßen vor:

1. Öffnen Sie aus dem Unterknoten **Einstellungen** die Einstellung **Lizenz**.
2. Auf dem Reiter **Lizenzen** tragen Sie Ihre erworbenen Lizenzen ein. Entweder geschieht dies direkt über das Hinzufügen einer Lizenzdatei oder eines Lizenzschlüssels, je nach dem was Ihnen vorliegt. Ein Assistent begleitet Sie durch die Aktivierung.



3. Sobald die Lizenz im System eingetragen ist, werden auf dem Reiter **Module** Ihre lizenzierten DriveLock Module angezeigt.
4. Selektieren Sie alle und klicken Sie auf die Schaltfläche **Bearbeiten**.
5. Im nächsten Dialog geben Sie an, wo die Module verfügbar sein sollen. Klicken Sie auf **Hinzufügen** und wählen Sie aus der Liste **< Alle Computer >**.

> Hinweis: Sie können hier auch andere Einstellungen vornehmen und die Module auf einzelne Computer, Gruppen oder OUs einschränken. Weitere

Informationen hierzu finden Sie im Administrationshandbuch auf DriveLock Online Help.

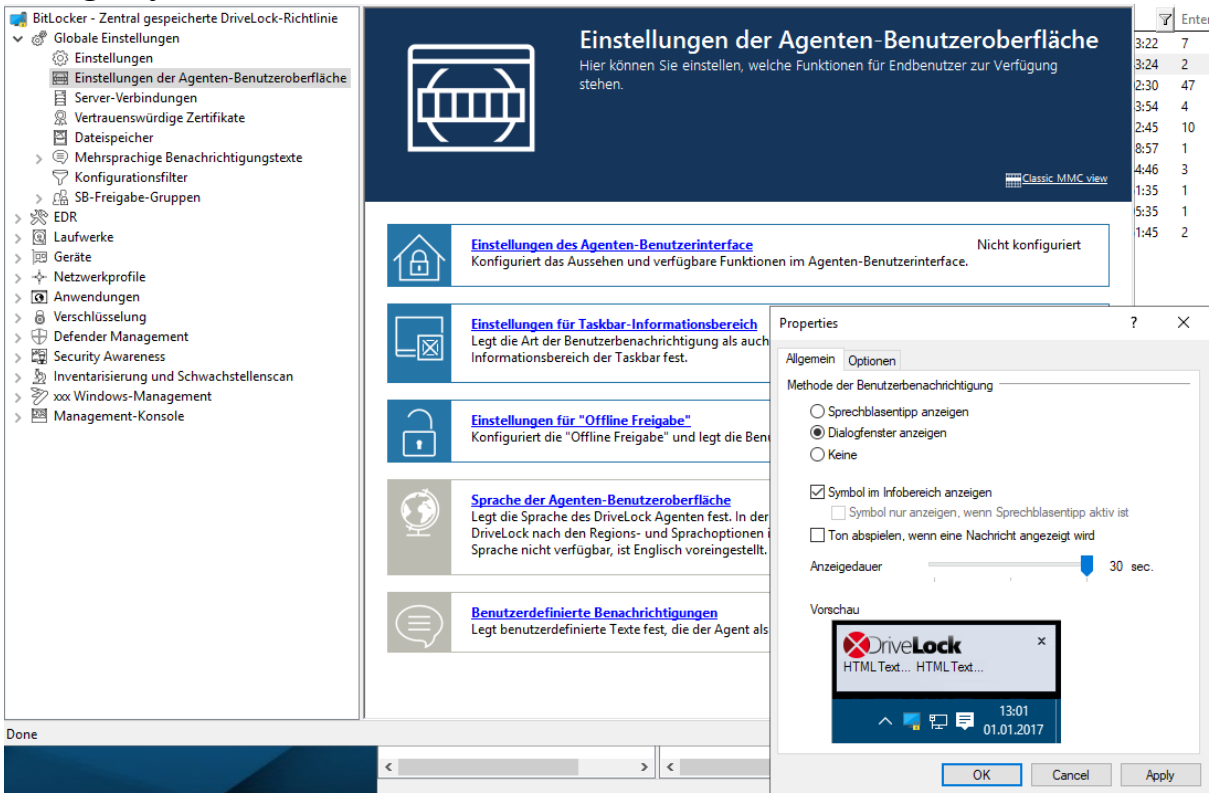
6. Bestätigen Sie Ihre Auswahl und speichern Sie Ihre Lizenzeinstellungen.

Hinweis: Um die von Ihnen nicht lizenzierten Module in der Richtlinie auszublenden, wählen Sie den Kontextmenübefehl **Nicht lizenzierte Knoten ausblenden** auf oberster Ebene der Richtlinie.

4.4.1.2 Einstellungen der Agenten-Benutzeroberfläche

Damit auf dem Client-Computer erkennbar ist, dass der DriveLock Agent aktiv ist, sollten Sie folgende Einstellung setzen:

1. Öffnen Sie im Knoten **Einstellungen der Agenten-Benutzeroberfläche** die **Einstellungen für den Taskbar-Informationsbereich**.
2. Wählen Sie auf dem Reiter **Allgemein** die Option **Symbol im Infobereich anzeigen** und dann eine der beiden Optionen **Dialogfenster anzeigen** oder **Sprechblasentipp anzeigen**, je nachdem, auf welche Art Sie die Benutzer informieren wollen.



3. Bestätigen Sie Ihre Einstellungen mit **Übernehmen** und **OK**.

4.4.2 Richtlinie speichern und veröffentlichen

Richtlinienänderungen sollten immer gespeichert und veröffentlicht werden.

Speichern  : Änderungen werden für DriveLock-Administratoren gespeichert.

Veröffentlichen  : Die Richtlinie wird gespeichert und als aktuell aktive Version an alle Agenten veröffentlicht.

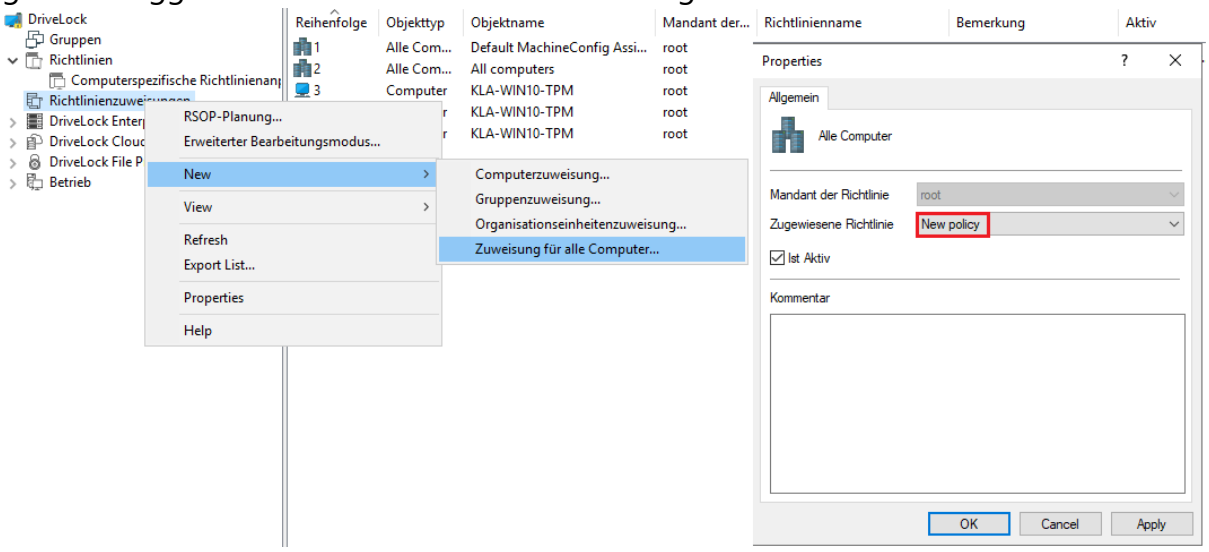
4.4.3 Richtlinie zuweisen

Zentral gespeicherte Richtlinien müssen manuell zugewiesen werden, damit eine Beziehung zwischen Richtlinie und DriveLock Agent auf einem (oder mehreren) Client-Computern hergestellt werden kann. Zuweisungsziele können alle oder einzelne Computer, Gruppen oder Organisationseinheiten sein.

Im Administrationshandbuch finden Sie hierzu ausführliche Erläuterungen. Im Zuge der Erstinstallation weisen Sie Ihre neue Richtlinie zunächst allen Computern zu.

Gehen Sie folgendermaßen vor:

1. Öffnen Sie im Knoten **Richtlinienzuweisungen** aus dem Kontextmenü den Befehl **Neu**.
2. Wählen Sie **Zuweisung für alle Computer...**.
3. Wählen Sie im Dialog als **Zugewiesene Richtlinie** Ihre neu erstellte Richtlinie aus, geben Sie ggf. einen Kommentar ein und bestätigen Sie mit **OK**.



4. Ihre Richtlinie steht jetzt zur Zuweisung bereit.

4.5 Erste Anmeldung am DriveLock Operations Center

Öffnen Sie das DriveLock Operations Center (DOC) über den Startmenü-Eintrag **DriveLock Operations Center Weblink**.

Beachten Sie bei der Anmeldung folgendes:

- Es können sich nur AD-Benutzer anmelden.
- Da SSL-Zertifikate verwendet werden, kann es unter Umständen zu Warnungen kommen.
- Sie können bereits an dieser Stelle die Sprache ein- bzw. umstellen.
- Jeder DriveLock Benutzer, der volle Helpdesk-Berechtigungen hat, kann sich mit seinem jeweiligen Kennwort anmelden.
- Die AD-Gruppe für die administrativen Benutzer kann in der Ansicht Einstellungen unter Konten eingetragen werden.

5 Installation des DriveLock Agenten

Auf jedem Client-Computer muss ein DriveLock Agent installiert sein, um dort die Zugriffe auf Geräte, Laufwerke, Dateien oder Applikationen kontrollieren und Verschlüsselungseinstellungen verteilen zu können. Der DriveLock Agent wird als MSI-Paket bereitgestellt, wobei ein Paket für 32-Bit- und ein weiteres für 64-Bit-Systeme vorhanden ist. Wählen Sie das richtige Paket anhand der Windows-Version auf den Client-Computern aus.

> Hinweis: Die MSI-Pakete für den DriveLock Agenten befinden sich auf der DriveLock ISO-Datei oder werden durch den DriveLock Installer aus dem Internet heruntergeladen. In der Management Konsole sind die Pakete im Knoten **Produkt-Pakete und -Dateien** unter **Softwarepakete** zu finden.

Grundsätzlich kann das MSI-Paket entweder manuell oder automatisiert installiert werden. Eine manuelle Installation ist für Testsysteme empfohlen, in allen anderen Fällen sollte eine automatisierte Installationsmethode gewählt werden.

Wenn kein Software-Verteilungssystem vorhanden sein sollte, bietet der DriveLock Enterprise Service die Möglichkeit, DriveLock Agenten auf alle oder einzelne Client-Computer im Netzwerk zu verteilen. Eine vollautomatische Push-Installation kann über das DriveLock Operations Center erfolgen.

Wenn Sie das Agenten-MSI-Paket mit einem Software-Verteilungssystem verteilen, muss es zunächst angepasst werden, um sicher zu stellen, dass jeder DriveLock Agent sofort nach der Installation die richtige Richtlinie erhält. Dies kann auf mehrere Arten erfolgen:

- Durch das Erstellen eines modifizierten Windows-Installationspakets (MSI-Datei) oder einer Windows Installer-Transformation (MST-Datei)
- Durch die Verwendung von Windows Installer-Kommandozeilenparametern.

5.1 Installationsvoraussetzungen für den DriveLock Agenten

Genaue Angaben zu den unterstützten Versionen und den Installationsvoraussetzungenfür den DriveLock Agenten finden Sie in den aktuellen Release Notes auf DriveLock Online Help.

5.2 Agentenverteilung über MSI

Gehen Sie folgendermaßen vor:

1. Öffnen Sie in der DriveLock Management Konsole im Knoten **Richtlinien** aus dem Kontextmenü **Alle Aufgaben** den Menübefehl **Zentral gespeicherte Richtlinie verteilen...**.
2. Starten Sie den Assistenten für die Agentenverteilung. Der Assistent fragt alle benötigten Parameter ab und generiert die entsprechende Ausgabe.
3. Wählen Sie im zweiten Dialog die zentral gespeicherte Richtlinie, die Sie erstellt haben und die von den DriveLock Agenten verwendet werden soll und den Server, auf dem der zentrale DriveLock Enterprise Service installiert ist.
4. Wählen Sie im nächsten Dialog die Art des Installationspakets, das vom Assistenten erstellt werden soll:
   - Microsoft Installer Datei (MSI): Erstellt ein neues Microsoft Installer Paket, das die zuvor spezifizierten Einstellungen enthält.
   - Microsoft Installer Transform Datei (MST): Erstellt eine Microsoft Installer Transform (MST) Datei mit den gewählten Einstellungen. Eine MST-Datei kann zusammen mit dem Original-MSI-Paket verwendet werden, das in der DriveLock Installation enthalten ist.
   - Kommandozeile: Zeigt die Kommandozeilen-Syntax mit den gewählten Einstellungen für den Microsoft Installer an.
5. Geben Sie Pfad und Name der Original-DriveLockAgent.msi-Datei und die neue MSI-Datei an.
6. Starten Sie die Agentenverteilung.

5.2.1 Installation über Kommandozeile

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

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

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

Nachfolgendes Beispiel zeigt eine Installation mit eigenen Parametern:

```
msiexec /i DriveLockAgent.msi /qn USECONFIGFILE=1 CONFIGFILE-
E="\\fileserver\share\drivelock.cfg" USESVCACCT=1 SVCACCOUNT-
T=domain\user
SVCPASSWORD="UCXUUZXY5LJLTJ2BAFPZTZ42JKBKPYCKCLVUXBEYYH2K6OZA"
```

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

`USESERVERCONFIG=1`	Angabe, dass eine zentral gespeicherte Richtlinie zum Einsatz kommt.
`CONFIGID=<GUID>`	`<GUID>` ist die GUID der zentral gespeicherten Richtlinie in der Form: XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX
`CONFIGSERVER=<name>`	`<name>` ist der Servername, auf dem der DriveLock Enterprise Service installiert wurde und von dem die Richtlinie geladen werden soll
`TENANTNAME=<tenant>`	`<tenant>` ist der Mandanten-Name, für den die Richtlinie gelten soll. Haben Sie keine Mandanten konfiguriert, verwenden Sie bitte „root“ als Mandanten-Name.
`USEPROXY=1`	Angabe, dass ein Proxy verwendet werden soll

`PROXY=named;<proxy>:<port>`
`PROXY=pac;<pac url>`
`PROXY=netsh`
	`<named>`: bestimmten Proxy verwenden
	`<pac>`: Proxy Auto Configuration Script mit URL verwenden
	`<netsh>`: System-Proxy verwenden, der mit netsh gesetzt ist

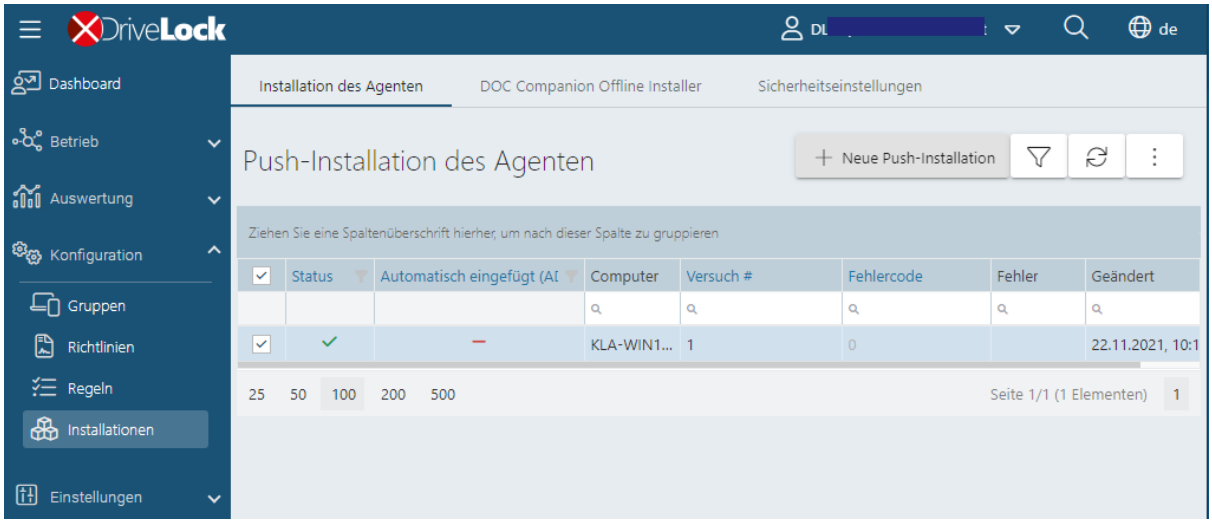
`PROXYACCOUNT=<authscheme>;`
 	
`<proxyuser>;<proxypassword>`
	Angabe eines Kontos, wenn der Proxy eine Authentifizierung verlangt.
	
	`<proxyuser>`: Benutzer
	
	`<proxypassword>`: Kennwort
	
	`<authscheme>`: mögliche Werte für das Authentifizierungsschema sind `basic, ntlm, passport, digest, negotiate`.

.

5.3 Push-Installation über das DOC

Diese Art der Installation eignet sich besonders für Testinstallationen und Reparaturen.

Gehen Sie folgendermaßen vor:

1. Öffnen Sie das DriveLock Operations Center (DOC).
2. Wählen Sie aus dem Menü auf der linken Seite die Ansicht **Konfiguration**.
3. In dieser Ansicht wählen Sie **Installationen** und dann den Reiter **Installation des Agenten**.
4. 

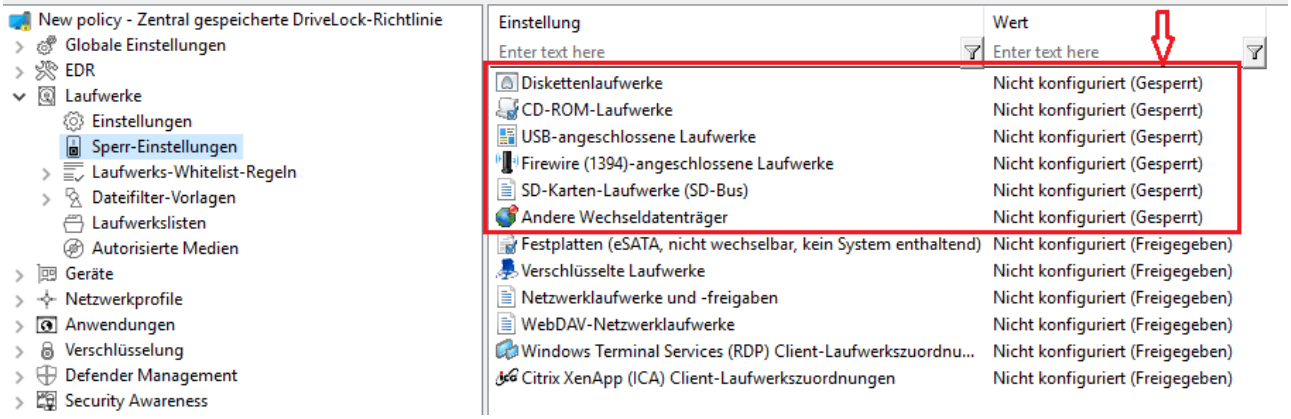
5. Geben Sie Ihren DES an und den Namen des Client-Computers, auf dem Sie den Agenten installieren wollen. Wiederholen Sie den Vorgang, um mehrere Computer hinzuzufügen.

6. Die Push-Installation kann einige Zeit in Anspruch nehmen. Sobald sie erfolgreich durchgeführt wurde, wird der Status des Computers mit einem grünen Häkchen gekennzeichnet.

5.4 Gesperrte Laufwerke auf dem Agenten nach der Installation

Beachten Sie, dass in den Standard-Einstellungen einer neuen Richtlinie der Zugriff auf folgende Laufwerke auf dem DriveLock Agenten gesperrt ist. Sie können diese Einstellungen jederzeit ändern.

> Achtung: Sobald der DriveLock Agent auf den Client-Computern installiert und somit die Richtlinie mit diesen Einstellungen wirksam ist, können Benutzer keine USB-Sticks oder andere Laufwerke mehr verbinden.

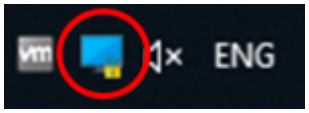


Mit Laufwerks-Whitelist-Regeln kann der Zugriff auf bestimme Laufwerke erlaubt werden. Alternativ können in der Richtlinie im Bereich Laufwerke die Zugriffsrechte konfiguriert werden. Details finden Sie im Administrationshandbuch auf DriveLock Online Help.

5.5 Überprüfung des DriveLock Agenten

Auf dem Client-Computer können Sie die Installation und den Zustand des Agenten folgendermaßen überprüfen:

- Suchen Sie das DriveLock-Agentensymbol in der Windows-Systemleiste.

  Wenn Sie das Kontextmenü öffnen, können Sie sich hier auch den **Agentenstatus** anzeigen lassen.

- Öffnen Sie die Benutzeroberfläche des DriveLock Agenten. Auf dem Reiter **Status** können Sie den Konfigurationsstatus des Agenten einsehen, indem Sie auf das entsprechende Symbol klicken.

- Prüfen Sie unter Dienste, ob DriveLock und DriveLock Health Monitor aktiv sind. Beide Dienste müssen laufen.

Sie können auch folgende Kommandozeile verwenden:

- `sc query drivelock` und/oder `sc query dlhm`: um nach den DriveLock-Diensten zu suchen
- `drivelock -showstatus`: um den Status der Agentenkonfiguration zu überprüfen

Bei Verwendung der Push-Installation:

- Überprüfen Sie das Windows-Ereignisprotokoll auf Meldungen des Dienstes "DLUpdate". Dieser Dienst protokolliert alle Fehler, die während der Installation aufgetreten sind, im Anwendungsprotokoll. Zusätzlich wird eine Protokolldatei der Push-Installation in "c:\windows\dlupdatexxx.log" geschrieben (xxx wird durch das aktuelle Datum und die Uhrzeit ersetzt).

Überprüfung im DOC

- In der Ansicht **Computer** wird Ihnen der Agenten-Status mit allen verfügbaren Eigenschaften angezeigt

6 Aktualisierung von DriveLock

> Hinweis: Zusätzliche Informationen zur Aktualisierung von DriveLock finden Sie in den aktuellen Release Notes auf DriveLock Online Help.

Es ist nicht notwendig, eine ältere Version von DriveLock zu deinstallieren, das Update wird automatisch durchgeführt, indem ein neueres Paket "über" die ältere Version installiert wird. Bei einem Update führen Sie die gleichen Schritte aus, die in den Kapiteln Installation der Komponenten, Installation des Servers und Installation der Datenbank beschrieben sind.

> Hinweis: Aktualisieren Sie als erstes den DriveLock Enterprise Service (DES) und erst danach alle anderen Komponenten.

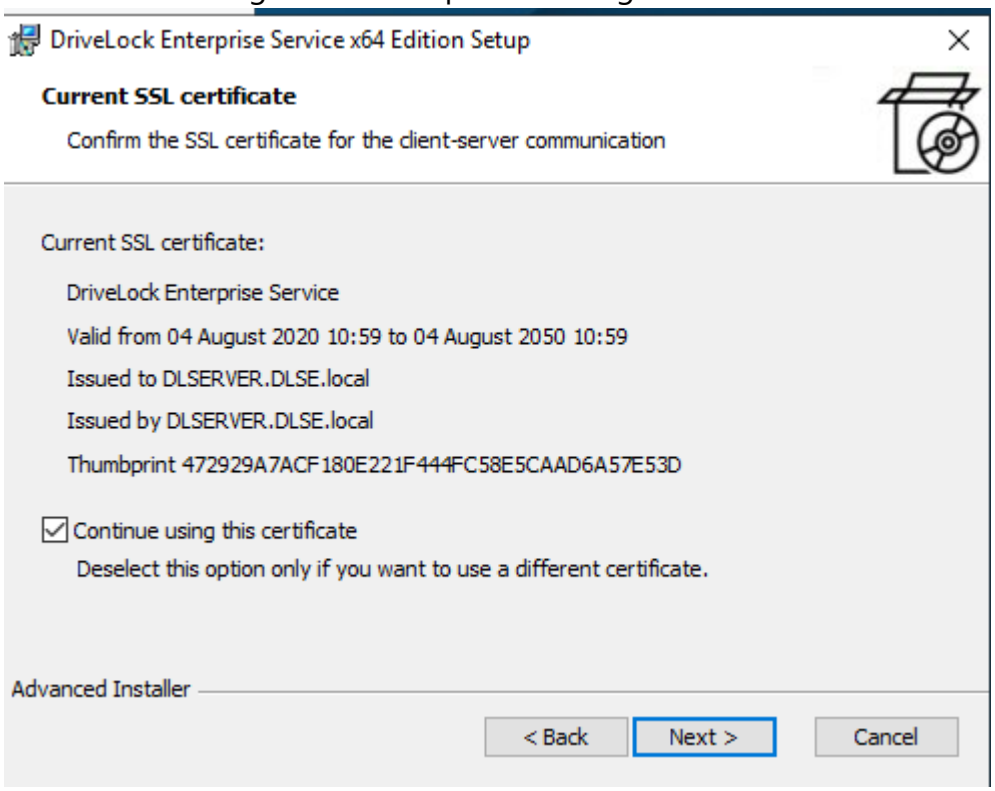
Beachten Sie dabei bitte folgende Unterschiede:

6.1 DriveLock Enterprise Service aktualisieren

Beachten Sie bitte folgendes:

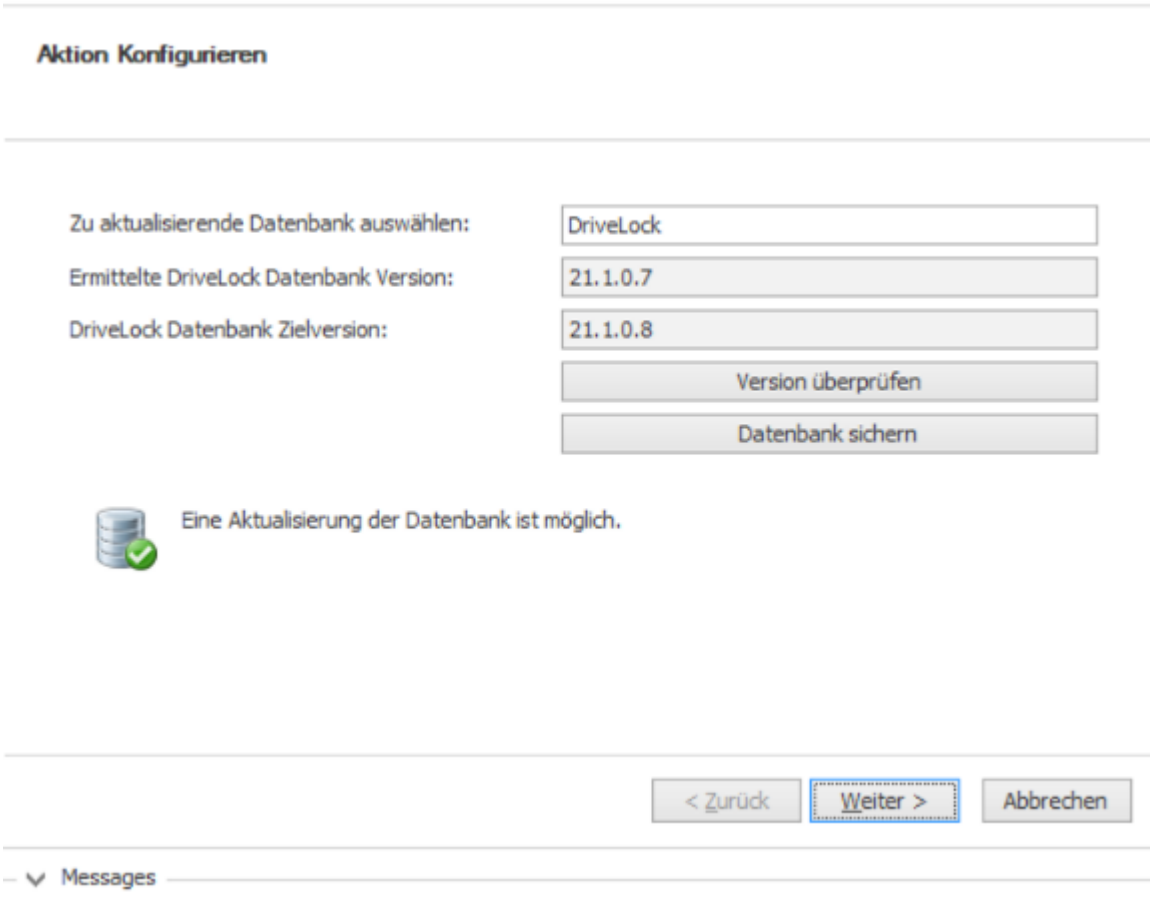
1. Aktualisieren Sie den DES vor der Aktualisierung der DriveLock Management-Komponenten.
2. Bevor Sie die Aktualisierung starten, benötigen Sie eine gültige Lizenz inklusive Wartung. Sie können diese in Ihrem aktuellen DriveLock Operations Center (DOC) erneuern. Wenn Sie Fragen zu Ihrer Lizenz haben, kontaktieren Sie bitte den DriveLock Support.
3. Bestätigen Sie das Zertifikat, das Sie für die Kommunikation zwischen DriveLock Management Konsole bzw. den DriveLock Agenten und dem DES ausgewählt haben. Ein

zusätzlicher Dialog im DES Setup Wizard zeigt Ihnen das Zertifikat an:



6.2 Datenbank aktualisieren

Bei der Aktualisierung der Datenbank durchlaufen Sie zunächst auch den Datenbank-Installationsassistenten. Nach dem Verbindungstest wählen Sie jedoch die Option **Eine bestehende DriveLock Datenbank überprüfen / aktualisieren**. Im Anschluss erscheint folgender Dialog, in dem die Datenbankversionen angezeigt werden:



6.3 DriveLock Agent aktualisieren

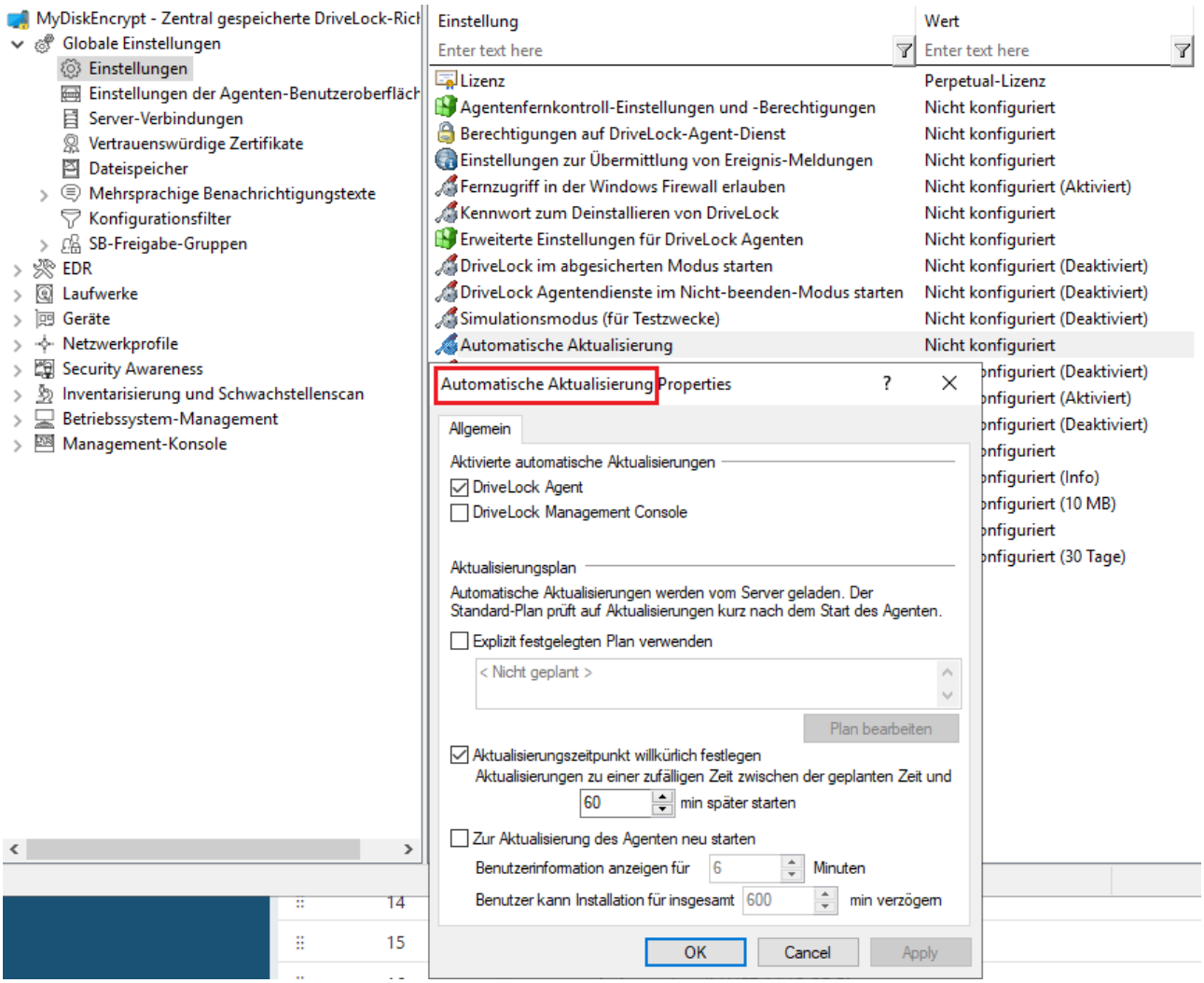
Hinweis: Die Version des DriveLock Agenten darf kleiner, aber nie größer sein als die Version des DriveLock Enterprise Services. Wir empfehlen, dass alle DriveLock Komponenten dieselbe Version haben.

Manuelle Installation

Sie können das neue Update manuell installieren. In diesem Fall installieren Sie einfach das neue Windows-Installationspaket (MSI). Es ist nicht notwendig, eine Agentenkonfiguration vorzunehmen, da die bestehende Konfiguration während des Updates erhalten bleibt.

Automatische Installation

Der DriveLock Agent kann automatische Updates durchführen. Diese Option ist standardmäßig in folgender Einstellung in der DriveLock Richtlinie aktiviert:



Der Agent prüft die veröffentlichten Softwarepakete auf dem DES auf eine neuere Version. Wenn eine neuere Version verfügbar ist, wird sie heruntergeladen und installiert.

Wenn Sie eine neue Version auf dem DES veröffentlicht haben und ein automatisches Update auslösen möchten, können Sie die Kommandozeile "`drivelock -updateproduct`" auf dem Agenten-Rechner verwenden.

Hinweis: Bitte beachten Sie auch die Hinweise zur Aktualisierung des Agenten in den aktuellen Release Notes auf DriveLock Online Help.

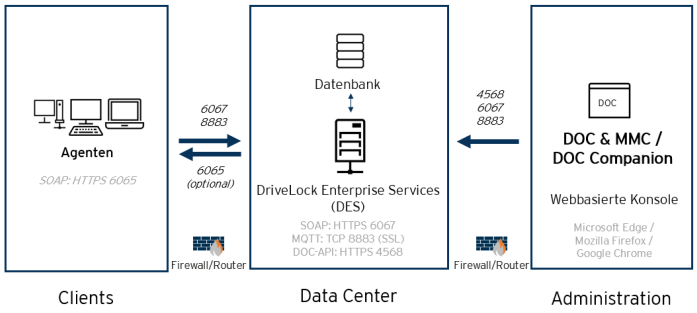
7 Anhang

7.1 DriveLock Architektur - On-Premise

Der zentrale DriveLock Enterprise Service (DES) benötigt eine Datenbank, um die Konfiguration und Rückmeldungen der Agenten zu speichern.

Sie können zudem verknüpfte DES verwenden, die nicht direkt auf die Datenbank zugreifen, sondern mit ihr über den zentralen Server interagieren. In großen DriveLock-Umgebungen kann so die Nutzung von Systemressourcen und Netzwerkbandbreite des zentralen DES reduziert werden.

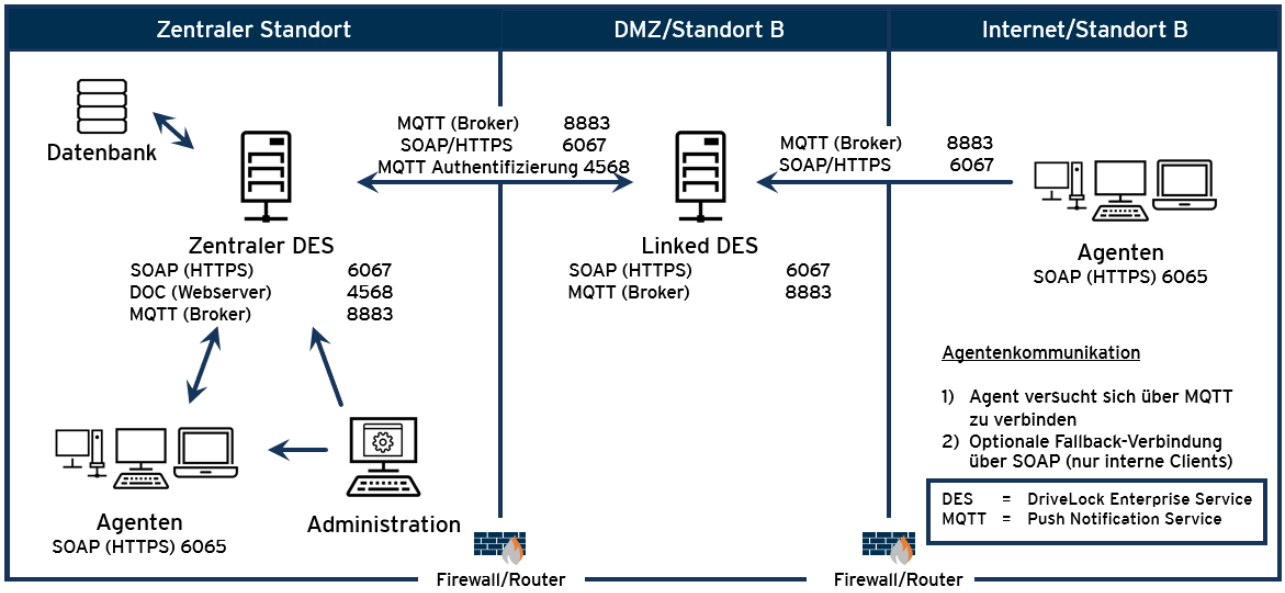
- Architektur mit zentralem DES:



- Architektur mit verknüpftem DES und Ports finden Sie hier:

7.1.1 Netzwerkkommunikationsstruktur und Ports

In der folgenden Abbildung sehen Sie die Netzwerkkommunikation zwischen den verschiedenen DriveLock Komponenten, inklusive der dazu verwendeten Ports:



Liste der benötigten Ports:

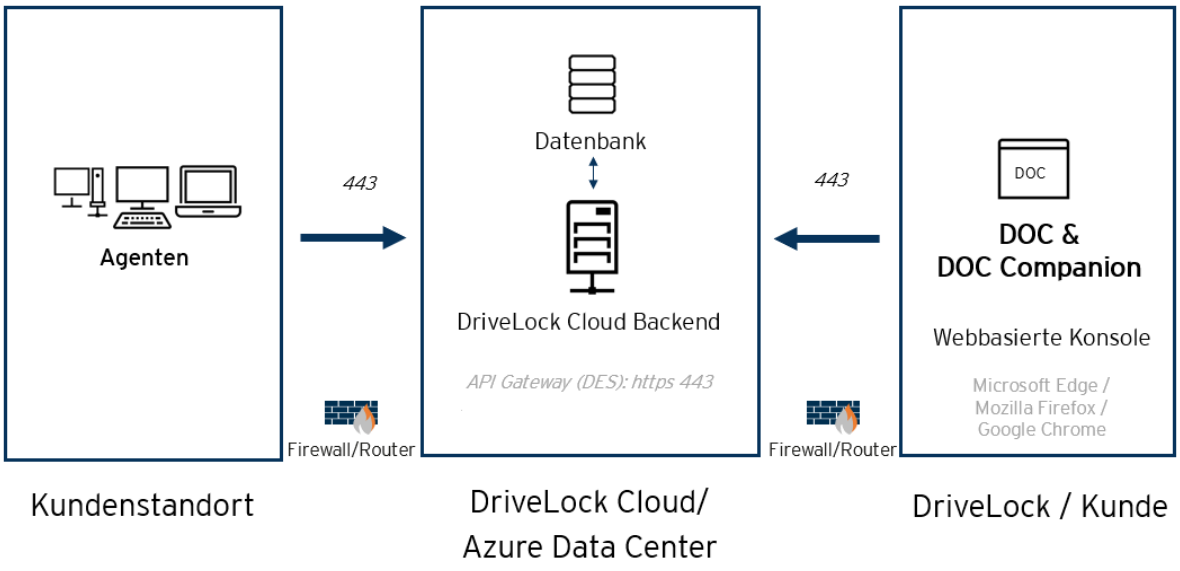
Datenbank:	
MSSQL-Ports	1433/1434
Übertragungsprotokoll HTTP:	
DES	6066
DriveLock Agent	6064
Übertragungsprotokoll HTTPS:	
DES	6067
DriveLock Agent	6065
Netzwerkprotokolle:	
MQTT (Broker)	8883

DOC (Webserver) / MQTT Authentifizierung	4568
LDAP	389

Achtung: Bitte beachten Sie, dass DriveLock keinerlei Änderung des MQTT-Ports unterstützt! Wenn der entsprechende Port bereits von einer anderen Anwendung verwendet wird, muss diese geändert oder entfernt werden, oder Sie müssen den DES auf einem anderen Server installieren.

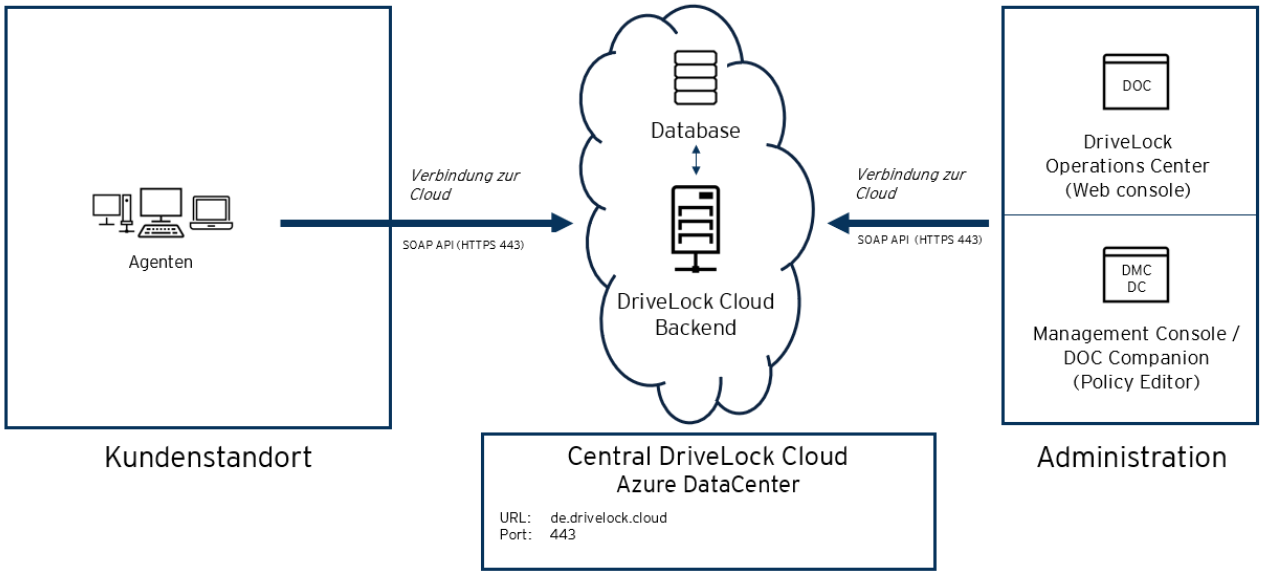
7.2 DriveLock Architektur - Cloud

Die Architektur im Cloud-Umfeld sieht folgendermaßen aus:



7.2.1 Kommunikationsstruktur und Ports

Wenn Sie Ihre DriveLock-Umgebung im Cloud-Umfeld aufgesetzt haben, sieht die Kommunikationsstruktur wie folgt aus:



7.3 Dateien, Verzeichnisse und Dienste für DriveLock

In Zusammenhang mit Antiviren-Software kann es unter Umständen notwendig sein, Ausschlüsse zu definieren.

Unter Umständen schlägt die Installation der DriveLock Disk Protection aufgrund einer Antivirus Software fehl, weil das ausgeblendete Verzeichnis `C:\SECURDSK` durch die Software in Quarantäne genommen wird. In diesem Falle sollten Sie für den Zeitraum der Installation den Virenschutz temporär ausschalten. Wir empfehlen, dieses Verzeichnis grundsätzlich als Ausnahme für den Virenscanner zu definieren.

Falls es zu weiteren unerwarteten Problemen mit Antiviren-Software kommen sollte, finden Sie im Folgenden eine Liste der ausführbaren Dateien, Verzeichnisse und Dienste, die von DriveLock verwendet werden:

Dateien und Verzeichnisse:

- "C:\SECURDSK" (EFS)
- "C:\Program Files\CenterTools\DriveLock" (Anwendungsverzeichnis)
- "C:\ProgramData\CenterTools DriveLock" (Cache/Arbeitsverzeichnis)

Prozesse/Dienste:

- **DriveLock**
  Anzeigename: DriveLock
  Ausführbarer Pfad: "C:\Program Files\CenterTools\DriveLock\DriveLock.exe"
- **dlhm**
  Anzeigename: DriveLock Health Monitor

Ausführbarer Pfad: "C:\Program Files\CenterTools\DriveLock\DLHM.exe"

- **StorageEncryptionService**
  Anzeigename: DriveLock Full Disk Encryption Encryptor
  Ausführbarer Pfad: "C:\Program Files\CenterTools\DriveLock\DlFdeEncSvc.exe"
- **ClientDataManager**
  Anzeigename: DriveLock Full Disk Encryption Manager
  Ausführbarer Pfad: "C:\Program Files\CenterTools\DriveLock\DlFdeMgr.exe"
- **dlupdate**
  Anzeigename: DriveLock Update and Installation
  Ausführbarer Pfad: "C:\Windows\DLUpdSvc.exe"
- **dessvc**
  Anzeigename: DriveLock Enterprise Service
  Ausführbarer Pfad: "C:\Program Files\CenterTools\DriveLock Enterprise Service\DES.exe"
- **DESTray**
  Funktion: Wird in der Taskleiste mit dem DES-Symbol angezeigt
  Ausführbarer Pfad: "C:\Program Files\CenterTools\DriveLock Enterprise Service\DESTray.exe"
- **DesRestarter**
  Funktion: Startet den DES-Dienst neu
  Ausführbarer Pfad: "C:\Program Files\CenterTools\DriveLock Enterprise Service\DesRestarter.exe"

7.4 Weitere Informationen zur Datenbankinstallation

An der Installation sind folgende Konten beteiligt:

- Das DES-Dienstkonto ist das Windows-Konto, unter dem der DES-Dienst läuft. Dieser wird bei der Installation angegeben und erhält durch die Installation Zugriff auf die Datenbank.
- Das Windows-Konto, das den DES installiert und lokale Administratorrechte hat. Dies ist in der Regel der angemeldete Benutzer, der die Installation durchführt.
- Das Konto für den Zugriff auf die Datenbank ist standardmäßig dasselbe Konto, das die Installation durchführt. Allerdings können Sie im Installationsassistenten auch eine andere Windows- oder SQL Server-Authentifizierung angeben.

Berechtigungen für die Datenbankinstallation

Das Konto, das für den Zugriff auf die Datenbank bei der Installation verwendet wird, benötigt folgende Berechtigungen:

SQL Server-Rollen:

- **dbcreator**: wird für das Anlegen der Datenbank benötigt
- **securityadmin**: wird für das Anlegen des Logins für den DES-Dienstkonto benötigt

Alternativ für Enterprise-Umgebungen:

- Das Anlegen der Datenbank und des Logins für das DES-Dienstkonto kann von einem SQL Server Administrator vorbereitet werden. Der Login, der bei der Installation verwendet wird, benötigt in diesem Fall dann nur die SQL Server Rolle **public** und muss Mitglied der **db_owner** Rolle in der DriveLock Datenbank sein.
- Bei der Installation kann ausgewählt werden, ob die Datenbank angelegt oder eine vorbereitete Datenbank verwendet wird. Ebenfalls kann man auswählen, ob der Login für den DES-Dienstkonto erstellt wird oder nicht. Dadurch können die benötigten Berechtigungen auf den SQL Server für den Installations-Login angepasst werden.
- Für nachfolgende Updates ist für den Installations-Login nur die Mitgliedschaft in der **db_owner** Rolle der DriveLock Datenbank wichtig.

Berechtigungen des DES-Dienstkontos auf der Datenbank

Für den Betrieb benötigt das DES-Dienstkonto folgende Rollenmitgliedschaften in der DriveLock Datenbank:

- **db_datareader**: Lesen von Daten
- **db_datawriter**: Schreiben von Daten
- **srcsystem**: eigene Rolle die von DriveLock installiert wird, erlaubt das Ausführen von Stored Procedures und das Verwenden von eigenen Tabellentypen.

Für Datenbankwartung (Indexpflege), Backups und Löschen von alten Daten benötigt der DES-Dienstkonto zusätzlich noch Rollenmitgliedschaft für **db_owner**. Dies ist optional und für den Betrieb mit SQL Server Express empfohlen, wo keine SQL Jobs für diese Aufgaben angelegt werden können. Bei der Installation kann ausgewählt werden, ob das DES-Dienstkonto diese Berechtigung bekommt.

Copyright