DriveLock Encryption

Dokumentation 2023.1

DriveLock SE 2023

Inhaltsverzeichnis

1 VERSCHLÜSSELUNG MIT DRIVELOCK 8

1.1 Lizenzeinstellungen 8

2 DRIVELOCK BITLOCKER MANAGEMENT 9

2.1 Allgemeines 9

2.1.1 Systemanforderungen 10

2.1.2 Algorithmen für DriveLock BitLocker Management 12

2.2 Einstellungen in Richtlinien 13

2.2.1 Verschlüsselungszertifikate 13

2.2.1.1 Verschlüsselungszertifikate erzeugen 13

2.2.2 Benutzerbezogene Agenteneinstellungen 16

2.2.3 Einstellungen für die Verschlüsselung 18

2.2.3.1 Reiter Allgemein 18

2.2.3.2 Reiter Verschlüsselungsschutz 21

2.2.3.3 Reiter Wiederherstellung 23

2.2.3.4 Reiter Ausführungsoptionen 25

2.2.4 Einstellungen für die Pre-Boot-Authentifizierung 27

2.2.4.1 Authentifizierungstyp 28

2.2.4.1.1 Option: DriveLock Pre-Boot-Authentifizierung 30

2.2.4.2 Kennwortoptionen 31

2.2.4.3 Anmelde-Methoden 34

2.2.4.4 Erscheinungsbild 36

2.3 Entschlüsselung 37

2.3.1 Verschlüsselte Festplatten entschlüsseln 37

2.4 Richtline überschreiben (BitLocker) 39

2.5 Beispielkonfiguration 41

2.6 Wiederherstellung 42

2.6.1 Wiederherstellung verschlüsselter Festplatten 42
2.6.1.1 Entsperren von BitLocker-verschlüsselten Datenpartitionen 44
2.6.2 Vorgehensweise im Richtlinien-Editor 46
2.6.3 Vorgehensweise im DOC 50
2.6.3.1 Wiederherstellung mit Schlüssel-ID 51
2.7 Übernahme 51
2.7.1 Übernahme bestehender BitLocker-Umgebungen 51
2.7.2 Nachträgliche Anpassung von BitLocker-Richtlinien 52
2.8 DriveLock Agent 54
2.8.1 Anmeldung an BitLocker 54
2.8.2 BitLocker Management auf Client-Computern (DriveLock Agent) 54
2.8.3 Verschlüsselung auf Client-Computern durchführen 55
2.8.3.1 Verschlüsselung verzögern 57
2.8.4 Datenpartition mit vorhandenem BitLocker übernehmen 59
2.9 BitLocker-Aktionen nachverfolgen 62
3 DRIVELOCK PRE-BOOT-AUTHENTIFIZIERUNG 63
3.1 Einstellungen für die Pre-Boot-Authentifizierung 64
3.1.1 Benutzer 65
3.1.2 Benutzersynchronisation 65
3.1.3 Benutzerlöschung 66
3.1.4 Netzwerk-Pre-Boot (UEFI) 67
3.1.5 Notfall-Anmeldung 67
3.1.6 Selbstlöschung 68
3.2 Einstellungen in der Listenansicht für die PBA 68
3.2.1 Änderungen der lokalen PBA-Konfiguration zulassen 68
3.2.2 PBA-Tastaturtreiber auswählen 69
3.2.3 SmartCard-Treiber in PBA laden 69

3.3 PBA-Einstellungen im DriveLock Operations Center (DOC) 69
3.4 Richtlinie überschreiben (DriveLock PBA) 70
3.5 Netzwerk-Pre-Boot-Authentifizierung (UEFI) 72
3.5.1 Netzwerk-Pre-Boot (UEFI) 73
3.5.2 Anwendungsfall 1: Automatische Anmeldung 75
3.5.3 Anwendungsfall 2: Netzwerkanmeldung für alle AD-Benutzer 77
3.5.4 Netzwerk-PBA-Einstellungen im DOC 78
3.6 Einstellungen für die Notfall-Anmeldung 79
3.7 DriveLock Agent 82
3.7.1 Installation der DriveLock-PBA auf dem DriveLock Agenten 82
3.7.2 Anmeldung an der DriveLock-PBA 83
3.7.3 Netzwerk-Preboot-Authentifizierung 86
3.7.4 Notfall-Anmeldung mit Wiederherstellungscode 88
3.7.5 Windows-Authentifizierung 91
3.7.6 BIOS Pre-Boot-Authentifizierung 91
3.8 DriveLock-PBA-Kommandozeilenprogramm 94
3.9 Abkürzungs- und Funktionstasten 96
4 DRIVELOCK BITLOCKER TO GO 99
4.1 Voraussetzungen für BitLocker To Go 99
4.2 Einstellungen in Richtlinien 100
4.2.1 Allgemeine Einstellungen für BitLocker To Go 101
4.2.2 Wiederherstellung verschlüsselter Laufwerke 102
4.2.2.1 Administrator-Kennwort 102
4.2.2.2 Zertifikatsbasierte Laufwerks-Wiederherstellung 103
4.2.3 Erzwungene Verschlüsselung 104
4.3 Beispielkonfiguration für eine Verschlüsselung mit BitLocker To Go 105
4.3.1 Laufwerks-Whitelist-Regel anlegen 107

4.4 BitLocker To Go-Wiederherstellung 108
4.4.1 Wiederherstellungsprozess 109
4.4.2 Wiederherstellung im DriveLock Operations Center (DOC) 110
4.5 DriveLock Agent 110
4.5.1 BitLocker To Go auf dem DriveLock Agenten 110
4.6 Verschiedene Anwendungsfälle 113
4.6.1 Administrator-Kennwort-Regeln 113
4.6.2 Verschlüsselungs-Regeln 114
5 DRIVELOCK ENCRYPTION 2-GO 115
5.1 Allgemeines 115
5.1.1 Verschlüsselungsverfahren 115
5.2 Einstellungen in Richtlinien 116
5.2.1 Einstellungen 116
5.2.1.1 Globale Einstellungen konfigurieren 117
5.2.1.2 Einstellungen für erzwungene Verschlüsselung 118
5.2.1.3 Einstellungen für die Kennwort-Wiederherstellung 119
5.2.1.4 Erweiterte Einstellungen 119
5.2.2 Wiederherstellung verschlüsselter Container 125
5.2.2.1 Administrator-Kennwort 125
5.2.2.2 Zertifikatsbasierte Container-Wiederherstellung 126
5.2.3 Erzwungene Verschlüsselung 126
5.2.3.1 Verschlüsselungs-Regel 127
5.2.3.2 Benutzerauswahl-Regel 129
5.3 Offline-Wiederherstellungsprozess 131
5.4 Online-Wiederherstellungsprozess 132
5.5 Wiederherstellung im DriveLock Operations Center (DOC) 134
6 DRIVELOCK FILE PROTECTION 135

6.1 Wie funktioniert DriveLock File Protection? 135
6.1.1 Unterstützte Verschlüsselungsverfahren 137
6.2 File Protection konfigurieren 137
6.2.1 Master-Zertifikat für die Schlüsselverwaltung einrichten 138
6.2.2 Zertifikatsverwaltung konfigurieren 139
6.3 Einstellungen in Richtlinien 140
6.3.1 Einstellungen zur Verschlüsselung konfigurieren 140
6.3.2 Benutzeroberfläche der Verschlüsselung konfigurieren 141
6.3.3 Einstellungen für verschlüsselte Laufwerke konfigurieren 143
6.3.4 Zusätzliche Einstellungen konfigurieren 144
6.3.5 Verwendetes Verschlüsselungsformat 145
6.4 Erzwungene Verschlüsselung 146
6.5 Wiederherstellung verschlüsselter Laufwerke konfigurieren 147
6.5.1 Unternehmenszertifikat 150
6.6 Benutzer und Zertifikate verwalten 151
6.6.1 Wie funktioniert die Benutzerverwaltung? 152
6.6.2 Benutzer verwalten 153
6.6.3 Gruppen verwalten 154
6.6.4 Zertifikate verwalten 155
6.7 Verschlüsselte Laufwerke zentral verwalten (Zentral verwaltete Ordner) 158
6.7.1 Vorbereitungen im Active Directory 158
6.7.1.1 Duplizieren der Zertifikatsvorlage 159
6.7.1.2 Ausstellen der Vorlage 162
6.7.1.3 Erstellen einer Gruppenrichtlinie 164
6.7.1.4 Automatische Registrierung 165
6.7.1.5 Testen der automatische Registrierung 168
6.7.2 Neues verschlüsseltes Laufwerk anlegen 169

6.7.3 Zugriffsberechtigungen ändern ... 170
6.8 Anwendungsfall: Zugriff auf verschlüsselte Ordner ... 172
6.9 Wiederherstellung verschlüsselter Verzeichnisse ... 179
6.10 File Protection im DOC ... 179
7 DRIVELOCK DISK PROTECTION ... 180
7.1 Einstellungen in Richtlinien ... 180
7.1.1 Verschlüsselungszertifikate ... 180
7.1.1.1 Verschlüsselungszertifikate erzeugen ... 182
7.1.1.2 Wiederherstellungsschlüssel ... 182
7.1.2 Benutzerbezogene Agenteneinstellungen ... 183
7.1.3 Einstellungen für die Verschlüsselung ... 185
7.1.4 Einstellungen für die Pre-Boot-Authentifizierung ... 187
7.1.4.1 Allgemein ... 187
7.1.4.2 Netzwerk-Pre-Boot (BIOS) ... 189
7.2 Entschlüsselung ... 189
7.3 Richtlinie überschreiben (Disk Protection) ... 190
7.4 DriveLock Disk Protection Wiederherstellung und Tools ... 192
7.4.1 Diagnoseinformationen speichern ... 193
7.4.2 Einstellungen für die Notfall-Anmeldung (Challenge-Response) ... 194
7.4.3 Wiederherstellung verschlüsselter Laufwerke ... 195
7.4.3.1 Disk-Schlüssel-Wiederherstellung ... 195
7.4.3.2 Erstellen eines Wiederherstellungsmediums ... 197
7.4.3.2.1 Windows PE-Wiederherstellungs-Assistent ... 197
7.4.3.3 Wiederherstellung der Festplatte ... 198
7.4.4 Fernlöschung ... 200
INDEX ... 202
COPYRIGHT ... 204

1 Verschlüsselung mit DriveLock

Mit der DriveLock Datenverschlüsselung und dem Zero Trust Sicherheitsansatz sind Sie auf der sicheren Seite. Dazu bietet DriveLock verschiedene Verschlüsselungsmodule:

- **DriveLock Disk Protection**

  Transparente und schnelle Festplattenverschlüsselung

- **DriveLock BitLocker Management**

  Festplattenverschlüsselung mit Microsoft BitLocker – ergänzt um wichtige Zusatzfunktionen

  > Hinweis: Die DriveLock Pre-Boot-Authentifizierung (PBA) kommt sowohl bei BitLocker Management, also auch bei Disk Protection zum Einsatz.

- **DriveLock BitLocker To Go**

  Verschlüsselung von Wechseldatenträgern mit Microsoft BitLocker To Go – ergänzt um wichtige Zusatzfunktionen

- **DriveLock Encryption 2-Go**

  Container-basierte Verschlüsselung von Wechseldatenträgern wie USB-Laufwerke, CD/DVD oder Wechselplatten

- **DriveLock File Protection**

  Datei-basierte Verschlüsselung von Verzeichnissen und Dateien

1.1 Lizenzeinstellungen

Um die verschiedenen Verschlüsselungsmodule nutzen zu können, benötigen Sie unterschiedliche Lizenzen. Die Lizenzeinstellungen sind im Richtlinien-Editor unter den globalen Einstellungen oder im DriveLock Operations Center unter Lizenzen zu finden.

> Hinweis: Allgemeine Informationen zur Lizenzierung finden Sie sowohl in den Dokumentationen zur Installation als auch zur Administration von DriveLock auf DriveLock Online Help.

> Achtung: Eine gleichzeitige Zuweisung der Disk Protection- und BitLocker Management-Lizenz in derselben Richtlinie ist nicht möglich!

2 DriveLock BitLocker Management

DriveLock BitLocker Management bietet Ihnen eine Reihe von Vorteilen gegenüber dem herkömmlichen Einsatz von Microsoft BitLocker:

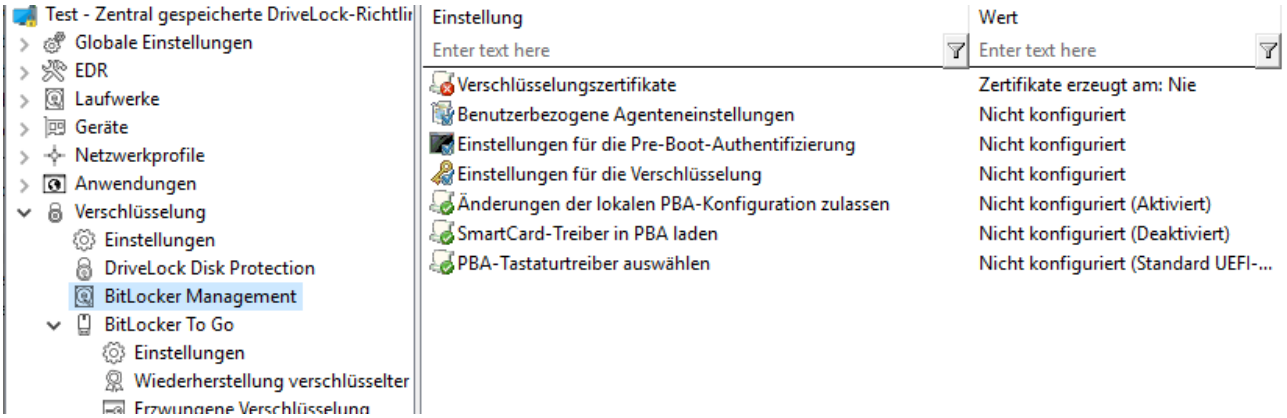
- Die Verschlüsselung mit der BitLocker-Technologie lässt sich von zentraler Stelle aus verwalten
- Sie behalten so die Übersicht über alle Client-Computer, deren Festplatten mit BitLocker verschlüsselt sind
- Bereits bestehende BitLocker-Umgebungen können in DriveLock BitLocker Management übernommen werden
- Es unterstützt neben den gängigen BitLocker Authentifizierungsmethoden auch Smartcard und Token.
- Sie können im DriveLock Operations Center (DOC) den Ver- und Entschlüsselungsstatus einzelner Geräte überwachen
- Es ermöglicht eine sichere und zentrale Verwaltung der BitLocker-Wiederherstellungsschlüssel
- Bei Verlust oder Diebstahl von Geräten kann eine Stilllegung bei erneuter Netzwerkverbindung schnell durchgeführt werden
- Es verhindert den unbefugten Zugriff bei außer Betrieb genommenen oder recycelten Endgeräten
- Mit der DriveLock Pre-Boot-Authentifizierung für BitLocker haben Sie die Möglichkeit, die Systempartition über Ihre Windows-Anmeldung zu entsperren. Dadurch entfällt die Eingabe des computerspezifischen BitLocker-Kennworts.

2.1 Allgemeines

BitLocker Management ermöglicht es Ihnen, die BitLocker-Verschlüsselung der Client-Computer in Ihrem Netzwerk von zentraler Stelle aus zu verwalten.

Sobald Sie BitLocker Management lizenziert, die Richtlinie gespeichert und neu geöffnet haben, wird in der entsprechenden Richtlinie im Knoten **Verschlüsselung** der neue Unterknoten BitLocker Management angezeigt. Hier können Sie alle Einstellungen für die Verschlüsselung, die Installation und die Authentifizierung vornehmen, sowie Verschlüsselungszertifikate erzeugen.

Hinweis: Wenn Sie BitLocker Management neu einsetzen, beginnen Sie als erstes mit der Erstellung der Zertifikate.



2.1.1 Systemanforderungen

Hinweis: Informationen zu allgemeinen Systemanforderungen (Hardware- und Betriebssystemvoraussetzungen) finden Sie in den aktuellen Release Notes auf DriveLock Online Help.

Achtung: In Ausnahmefällen kann es notwendig sein, dass die Festplatte mit der Boot-Partition zuvor für die Verwendung mit BitLocker vorbereitet werden muss. In diesem Fall führen Sie bitte die folgenden Schritte durch:
Prüfen Sie den Status mittels "manage-bde -status c:"
Sollte eine Fehlermeldung "ERROR: The volume C: could not be opened by BitLocker. This may be because the volume does not exist, or because it is not a valid BitLocker volume." angezeigt werden, muss die Festplatte vorbereitet werden. Siehe https://docs.microsoft.com/de-de/windows-server/administration/windows-commands/bdehdcfg. In einer Admin-Befehlszeile können Sie die Vorbereitung mittels "bdehdcfg.exe -target default" oder "bdehdcfg.exe -target default -restart -quiet" (ohne Nachfrage für Skripting) durchführen

DriveLock Bitlocker Management unterstützt folgende Betriebssysteme:

- **Windows 7**

  Achtung: Für Windows 7 wird ab DriveLock Version 2023.1 eine Legacy-Lizenz erforderlich.

  - ab Windows 7 SP1 (Version 6.1.7601)
  - nur 64-Bit Betriebssystem
  - nur Ultimate und Enterprise Edition

    - ein vorhandenes Trusted Platform Module (TPM Chip oder vTPM) ist zwingend erforderlich

- **Windows 8**
    - ab Windows 8.1, Update 1 (Version 6.3.9600)
    - 32-Bit und 64-Bit Betriebssysteme
    - nur Professional und Enterprise Edition
    - kein TPM erforderlich (für höhere Sicherheit aber empfohlen)
- **Windows 10 und höher**
    - ab Windows 10 1607 (Version 10.0.14393)
    - 32-Bit und 64-Bit Betriebssysteme
    - nur Professional, Enterprise und Education Edition
    - kein TPM erforderlich (für höhere Sicherheit aber empfohlen)

Achtung: Bitte beachten Sie, dass das BitLocker-Feature für Server-Betriebssysteme nicht standardmäßig installiert ist.

DriveLock PreBoot Authentication (DriveLock PBA) für Bitlocker unterstützt nur folgende Betriebssysteme:

- **Windows 10 und höher**
    - UEFI-Firmware erforderlich
    - 64-Bit Betriebssysteme
    - nur Professional, Enterprise und Education Edition
    - kein TPM erforderlich (für höhere Sicherheit aber empfohlen)

2.1.2 Algorithmen für DriveLock BitLocker Management

Zur Festplattenverschlüsselung verwendet BitLocker Management folgende Algorithmen, die sich nach dem eingesetzten Betriebssystem richten. Dabei werden die Methoden der jeweiligen Vorgängerversionen auch unterstützt. Siehe auch Kapitel Systemvoraussetzungen.

Betriebssystem	Algorithmus
Windows 7	• AES 128-bit mit Diffuser • AES 256-bit mit Diffuser • AES 128-bit • AES 256-bit
Windows 8.1	• AES 128-bit • AES 256-bit
Windows 10 und höher	• AES-XTS 128-bit • AES-XTS 256-bit

Hinweis: Bei Datenlaufwerken ist der Standardalgorithmus **AES 128** (dies ist der zu den meisten Betriebssystemen kompatible Algorithmus).

Hinweis: Achten Sie darauf, den passenden Algorithmus auszuwählen. Die oben genannten Standardalgorithmen sind hier die beste Wahl. Bei Übernahme von bestehenden BitLocker-Umgebungen hat die korrekte Auswahl Einfluss darauf, wie schnell DriveLock die Umgebungen ent- und wieder verschlüsseln kann.

2.2 Einstellungen in Richtlinien

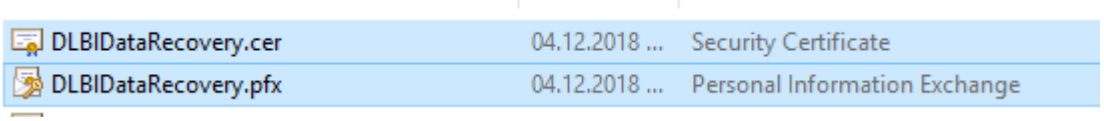
2.2.1 Verschlüsselungszertifikate

Um mit BitLocker Management eine Festplattenverschlüsselung durchführen zu können, benötigen Sie Verschlüsselungszertifikate. Diese braucht DriveLock zum Einen zur Verschlüsselung und zum Anderen für die Wiederherstellung (zur Bereitstellung des Wiederherstellungschlüssels und für eine eventuelle Notfall-Anmeldung).

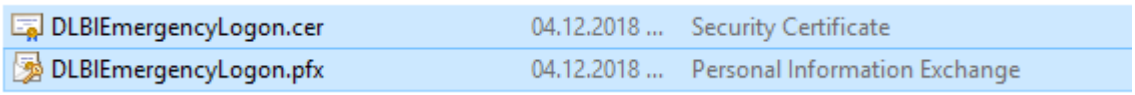
DriveLock fügt die Verschlüsselungszertifikate automatisch in den Windows Zertifikatsspeicher ein.

Hinweis: Die Verschlüsselungszertifikate müssen unbedingt an einem anderen sicheren Ablageort im Dateisystem oder auf einer Smartcard gespeichert werden.

Die BitLocker-Verschlüsselungszertifikate bestehen aus zwei Teilen, dem eigentlichen Zertifikat (in der Abbildung **DLBlDataRecovery.cer**) und dem privaten Schlüssel (in der Abbildung **DLBlDataRecovery.pfx**):



Das Zertifikat für die Notfall-Anmeldung besteht aus folgenden Teilen:



Achtung: Verhindern Sie ein Überschreiben dieser Zertifikate, da sie zur Systemwiederherstellung der Clients benötigt werden.

Wenn Sie eine neue Richtlinie erstellen, mit der Sie BitLocker Management steuern wollen (BitLocker-Richtlinie), erzeugen Sie zunächst neue Zertifikate. Gehen Sie dazu wie in Kapitel Verschlüsselungszertifikate für BitLocker Management erzeugen beschrieben vor.

2.2.1.1 Verschlüsselungszertifikate erzeugen

Gehen Sie folgendermaßen vor:

1. Sobald Sie Ihre BitLocker-Richtlinie erstellt und lizenziert haben, müssen Sie diese zunächst speichern und erneut öffnen. Dann erst sehen Sie den Unterknoten BitLocker Management.

> Hinweis: Eine Textmeldung zeigt an, dass noch keine Verschlüsselungszertifikate erzeugt worden sind.

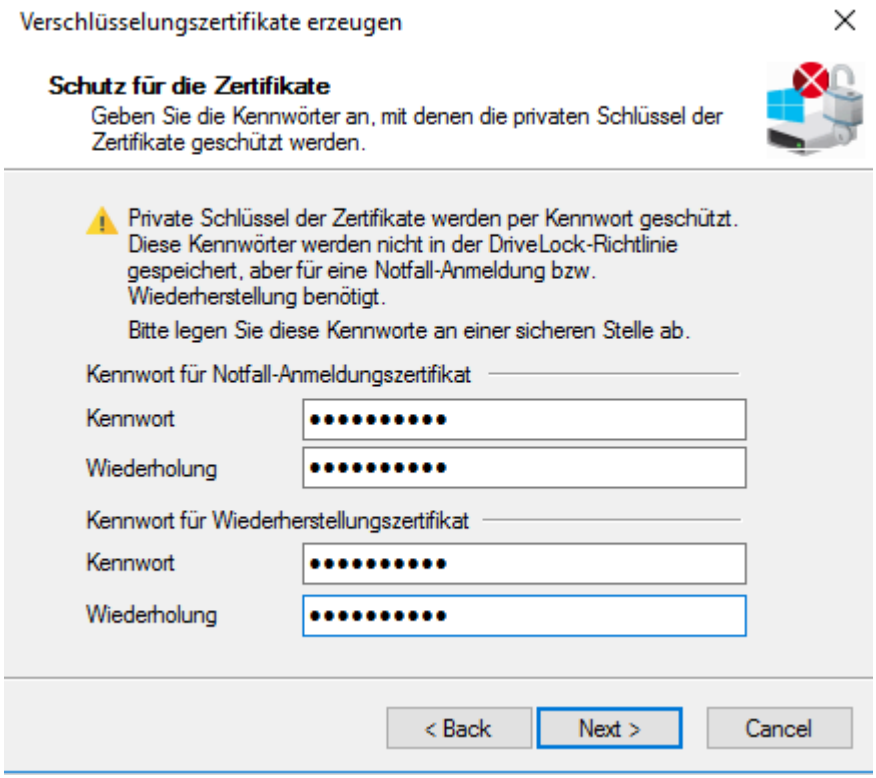
2. Klicken Sie auf die Schaltfläche **Verschlüsselungszertifikate** oder auf den Link in der Meldung.
3. Wählen Sie im nächsten Dialog die Schaltfläche **Zertifikate erzeugen**.

   Bereits existierende Zertifikate können importiert werden, indem Sie auf die Schaltfläche **Zertifikate verwalten** klicken. Sie müssen dabei jedoch sicherstellen, dass dadurch keine eventuell vorhandenen Zertifikate überschrieben werden und somit eine Wiederherstellung unmöglich gemacht wird.
4. Folgen Sie dem Assistenten und geben dann einen **Ablageort für die Zertifikate** an. Dies kann entweder ein Dateisystem-Ordner oder eine Smartcard sein.
   Sofern eine Smartcard zur Speicherung verwendet wird, werden Sie aufgefordert, die PIN für den Zugriff auf die Smartcard einzugeben.
   Die Option **Zertifikat auch in der Datenbank speichern (zur Verwendung im DOC)** ist standardmäßig gesetzt, damit Sie vom DriveLock Operations Center (DOC) aus Zugriff auf die Zertifikate haben.

   > Hinweis: Beachten Sie bitte bei dieser Angabe, dass entsprechende Sicherheitsvoraussetzungen erfüllt sind hinsichtlich Ablageort und Zugriff.

5. Im nächsten Schritt geben Sie Kennwörter ein, um die privaten Schlüssel zu schützen (s. Abbildung).

   > Hinweis: In diesem Dialog geben Sie sowohl das Kennwort für das Notfall-Anmeldungs- als auch für das Wiederherstellungszertifikat an.

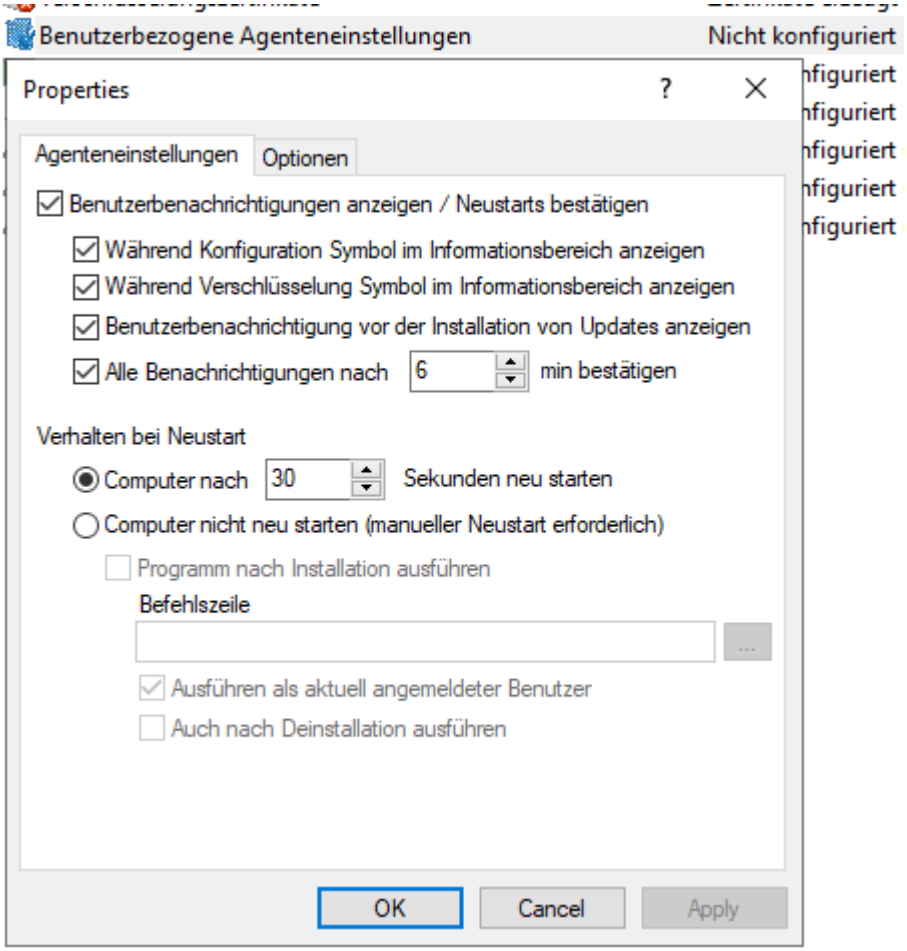


6. DriveLock erstellt nun die Verschlüsselungszertifikate an dem vorgegebenen Ablageort.

2.2.2 Benutzerbezogene Agenteneinstellungen

Standardmäßig werden Benutzer der DriveLock Agenten von der Installation von BitLocker Management bzw. der DriveLock PBA für BitLocker informiert und ihr Client-Computer wird nach der Installation nach 30 Sekunden neu gestartet. Sie können diese Einstellungen bei Bedarf ändern.

Reiter Agenteneinstellungen



Sie können dabei auswählen, ob Benachrichtigungen angezeigt werden und genau differenzieren, wann diese im Benachrichtigungsfeld angezeigt werden: während der Konfiguration, während der Verschlüsselung und bzw. oder vor der Installation von Updates.

Wählen Sie die Option **Computer nicht neu starten (manueller Neustart erforderlich)**, wenn Sie diesen selbst steuern wollen. Sie können dann z.B. über einen Kommandozeilenbefehl nach der Installation ein eigenes Installationsskript starten.

Hierfür stehen zwei Optionen zur Auswahl:

- **Ausführen als aktuell angemeldeter Benutzer**: Das Skript wird mit den Rechten des Benutzers ausgeführt, der gerade angemeldet ist. Standardmäßig läuft es sonst unter

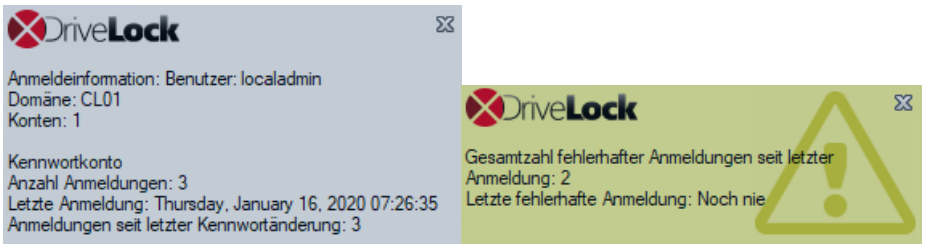
dem lokalen System.

- **Auch nach Deinstallation ausführen**: Das Skript wird nicht nur bei der Installation, sondern auch bei der Deinstallation ausgeführt.

Reiter Optionen

DriveLock BitLocker Management-Logon-Benachrichtigungen anzeigen: Wählen Sie diese Option aus, wenn die Anmelde-Informationen der Pre-Boot Authentifizierung nach der Anmeldung in Windows im Benachrichtigungsfeld des Client-Computers angezeigt werden sollen.

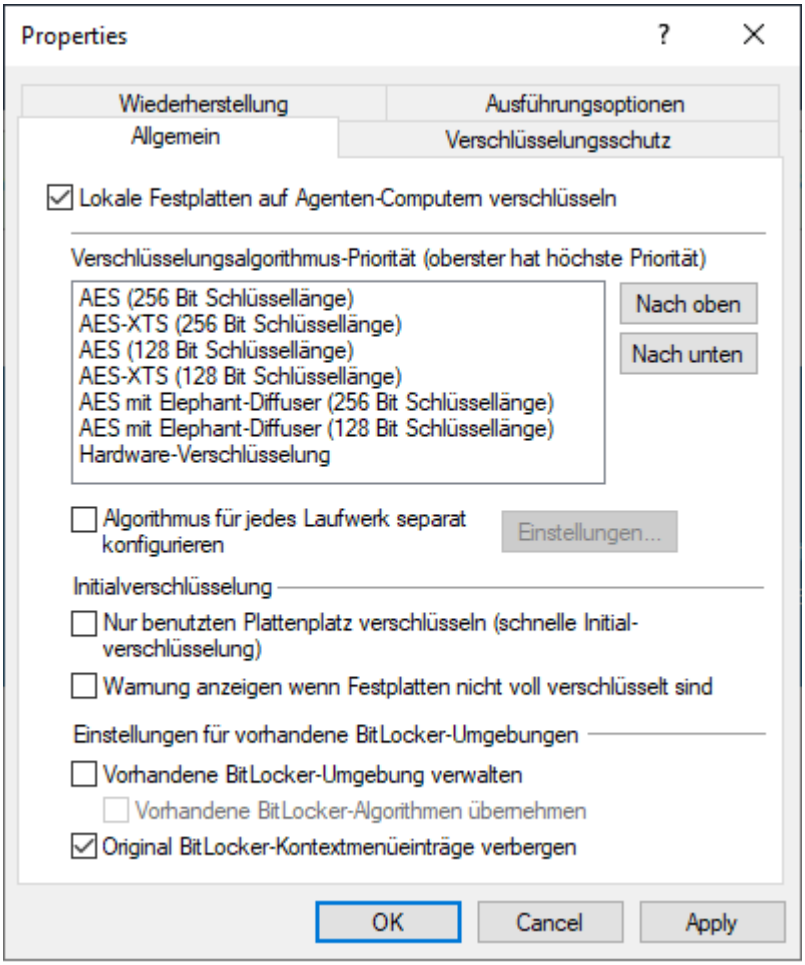
Auf dem Client-Computer erscheint dann eine Nachricht mit detaillierten Informationen (siehe Abbildung):



2.2.3 Einstellungen für die Verschlüsselung

2.2.3.1 Reiter Allgemein

Auf diesem Reiter stellen Sie die Werte für die Verschlüsselung und Entschlüsselung mit BitLocker ein.



Folgende Optionen stehen zur Wahl:

1. **Lokale Festplatten auf Agenten-Computern verschlüsseln**:
   - Wählen Sie diese Option, um die **Verschlüsselung** der Festplatten mit BitLocker zu starten. Alle anderen Einstellungen zur Verschlüsselung (wie weiter unten beschrieben) sollten Sie zu diesem Zeitpunkt festgelegt haben.

     Achtung: Sobald diese Option aktiviert wurde, die Richtlinie zugewiesen und am Client aktualisiert wurde, startet der Verschlüsselungsprozess!

   - Um eine **Entschlüsselung** zu erlauben (siehe detaillierte Beschreibung im Kapitel Entschlüsselung), muss das Häkchen entfernt werden und ggf. eine

Verzögerung in Tagen festgelegt werden.

> Achtung: Sobald Sie die Option deaktiviert und keine Verzögerung angegeben haben (und die Richtlinie zugewiesen ist und vom Client synchronisiert wurde), startet der Entschlüsselungsprozess!

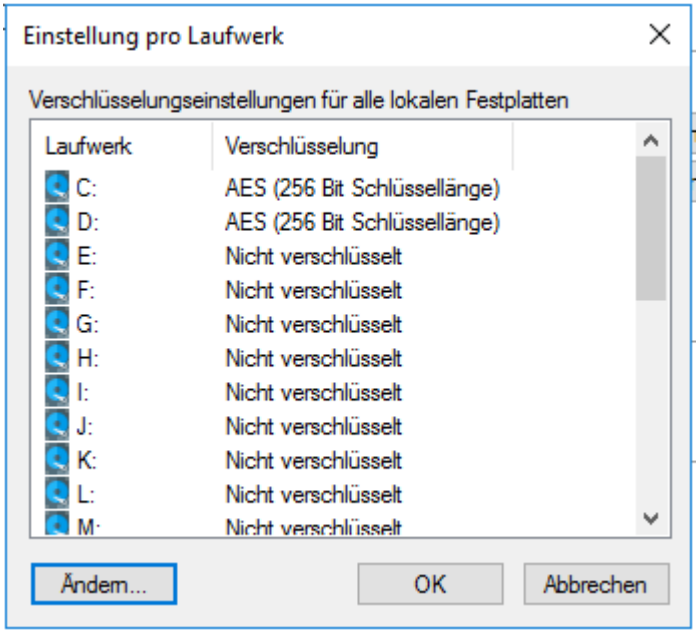
2. **Verschlüsselungsalgorithmus-Priorität**:
   - Die Liste der verschiedenen Verschlüsselungsmethoden wird von oben nach unten abgearbeitet. Sobald BitLocker Management einen passenden Algorithmus findet, der auf dem Client angewandt werden kann, wird dieser für die Verschlüsselung herangezogen.

> Hinweis: Der stärkste Algorithmus sollte immer an oberster Stelle stehen.

   - Sie können die Algorithmen auch manuell nach Ihren Vorgaben sortieren.
   - Algorithmus Hardware-Verschlüsselung:
     Dies ist ein individuell pro Festplatte eingebauter Verschlüsselungsalgorithmus, der je nach Hersteller variiert. Wenn Sie die Verschlüsselung auf entsprechend ausgestatteten Computern durchführen wollen, können Sie diesen Eintrag in der Liste nach oben schieben.
   - Beispiel:
     Wenn Sie viele Computer mit Windows 7 Systemen zu verschlüsseln haben, könnten Sie den Eintrag **AES mit Elephant-Diffuser (128 oder 256 Bit Schlüssellänge)** nach oben schieben, damit dieser Algorithmus bevorzugt wird.

3. **Algorithmus für jedes Laufwerk separat verschlüsseln**:
   - Wählen Sie hier für das Systemlaufwerk und die voraussichtlichen Datenlaufwerke über die Schaltfläche **Ändern** den gewünschten Verschlüsselungsalgorithmus oder ‚Nicht verschlüsselt', wenn keine Verschlüsselung gewünscht ist

> Hinweis: Beachten Sie bei dieser Einstellung, dass die Zuordnung Laufwerksbuchstabe und Systempartition bei allen Computern, denen diese BitLocker-Richtlinie zugewiesen wird, einheitlich ist.



Wenn Sie die Option **Verschlüsselungsstatus nicht verändern** auswählen, wird entweder der bereits existierende Algorithmus weiterverwendet oder das Laufwerk bleibt entschlüsselt.

4. **Initialverschlüsselung**
   - **Nur benutzten Plattenplatz verschlüsseln (schnelle Initialverschlüsselung)**
     - Wählen Sie diese Option, wenn Sie nur den benutzten Plattenplatz verschlüsseln wollen.
     - Hintergrund:
       Mit Windows 8 hat BitLocker ein Feature eingeführt, dass die Festplatte nicht komplett verschlüsselt werden muss, sondern nur der Teil, auf dem sich Daten befinden. Die initiale Verschlüsselung nimmt daher weniger Zeit in Anspruch.
     - Problem:
       Wenn Daten von der Festplatte gelöscht wurden und nicht mehr im Explorer sichtbar sind, können diese durchaus noch vorhanden sein und es kann mit entsprechenden Tools auf den ursprünglichen Bereich zugegriffen werden.

       Hinweis: Diese Option sollte nur dann aktiviert werden, wenn Sie beispielsweise neue Festplatten verschlüsseln wollen und sichergestellt ist, dass sich keine alten sicherheitsrelevanten Daten auf der Festplatte befinden. Ebenso ist diese Option bei allen SSD empfehlenswert.

- **Warnung anzeigen, wenn Festplatten nicht voll verschlüsselt sind**
  Bei jedem Reboot des Systems oder Neustart des DriveLock Agenten wird geprüft, ob alle Festplatten bereits gemäß den Einstellungen vollständig verschlüsselt sind. Wenn dies nicht der Fall ist, wird dem Benutzer ein entsprechender Hinweis angezeigt.

5. **Einstellungen für vorhandene BitLocker-Umgebungen**
   - **Vorhandene BitLocker-Umgebung verwalten**
     Aktivieren Sie diese Option, wenn Sie bereits bestehende BitLocker-Umgebungen mit DriveLock BitLocker Management verwalten wollen. Weitere Informationen finden Sie im Kapitel Übernahme bestehender BitLocker-Umgebungen.

     > Hinweis: Sobald Sie diese Option auswählen und die Richtlinie entsprechend zuweisen, öffnet sich an den Client-Computern, deren Datenlaufwerke noch mit original BitLocker verschlüsselt (und somit gesperrt) sind, ein Assistent zur Übernahme der Partitionen. Hier müssen Sie die Kennwörter der gesperrten Partitionen angeben, bevor die Übernahme erfolgen kann.

   - **Vorhandene BitLocker-Algorithmen übernehmen**
     Partitionen, die bereits mit BitLocker verschlüsselt sind, aber nicht dem in der Richtlinie definierten Algorithmus entsprechen, behalten den vorhandenen Algorithmus. Eine Neuverschlüsselung ist mit dieser Option nicht mehr nötig.
   - **Original BitLocker-Kontextmenüeinträge verbergen**
     Diese Option ist standardmäßig aktiviert. Alle BitLocker-Optionen im Windows-Startmenü oder -Explorer sind somit verborgen und die entsprechenden Dialoge werden nicht angezeigt. Die Möglichkeit, eine Festplatte oder ein Laufwerk versehentlich mit BitLocker aber ohne DriveLock zu verschlüsseln, ist somit stark eingeschränkt.

2.2.3.2 Reiter Verschlüsselungsschutz

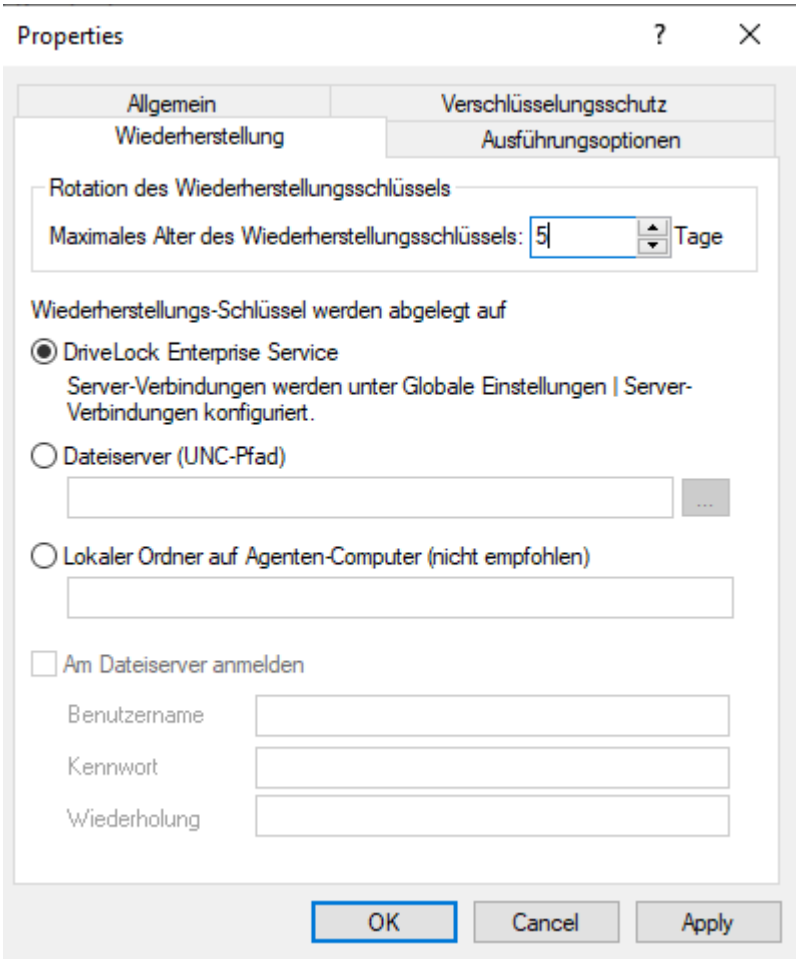
1. **Erst verschlüsseln, wenn Pre-Boot-Anmeldung einmal erfolgreich war**
   Das Setzen dieser Option ist eine Vorsorgemaßnahme, die das Verschlüsseln einerseits und die erste Anmeldung an der PBA andererseits trennt. Das Verschlüsseln wird so lange verzögert, bis die erste Anmeldung erfolgreich war.
2. **Verhalten bei Konfigurationsänderungen**

- **Entschlüsselung um [*x*] Tage verzögern**:
  Diese Einstellung zögert die Entschlüsselung um eine bestimmte Anzahl an Tagen hinaus. Dies kann sinnvoll sein, um die Client-Computer und deren Benutzer auf die Entschlüsselung entsprechend vorbereiten zu können.
  Als Standardwert ist ein Wert von **3** Tagen vordefiniert. Dieser Wert bietet einen zusätzlichen Schutz vor Fehlkonfigurationen. Wenn Sie sofort eine Entschlüsselung durchführen wollen, ändern Sie die Einstellung auf 0 Tage.
- **Keine Entschlüsselung durchführen**:
  Diese Option ist standardmäßig aktiviert. Sie führt dazu, dass es zu keiner ungewollten Entschlüsselung der BitLocker Verschlüsselung kommt, wenn Konfigurationsänderungen durchgeführt werden, z.B. bei Aktualisierung des DriveLock Agenten, bei Änderungen von Gruppenmitgliedschaften oder wenn die Richtlinie nicht mehr vom DriveLock Agenten angewendet wird.

> Achtung: Beachten Sie, dass eine Entschlüsselung nur durch Deaktivierung der oben beschriebenen Option **Lokale Festplatten auf Agenten-Computer verschlüsseln** angestoßen wird. Sobald der DriveLock Agent die so konfigurierte Richtlinie mit der expliziten Entschlüsselungseinstellung erhält, wird eine Entschlüsselung durchgeführt.

2.2.3.3 Reiter Wiederherstellung

Auf diesem Reiter geben Sie an, wo die verschlüsselten Wiederherstellungsdaten abgelegt werden sollen. Es handelt sich um die Einstellungen, die nach Starten des Wiederherstellungsprozesses auszuwählen sind.



Es stehen folgende Optionen zur Auswahl:

Rotation des Wiederherstellungsschlüssels

Mit der Einstellung **Maximales Alter des Wiederherstellungsschlüssels** in Tagen bestimmt man den Zeitraum für den regelmäßigen Wechsel des Wiederherstellungsschlüssels. Diese Option stellt sicher, dass der Wiederherstellungsschlüssel regelmäßig ausgetauscht wird. Dies verhindert eine missbräuchliche Verwendung des Wiederherstellungsschlüssels. Dabei bezieht sich die Angabe '1 Tag' auf 24 Stunden. Der Wiederherstellungsschlüssel wird nach dem Tausch sofort zum DES hochgeladen.

DriveLock Enterprise Service:

Wählen Sie diese Option, um die verschlüsselten Wiederherstellungsdaten an den DriveLock Enterprise Service (DES) zu schicken.

Dateiserver (UNC-Pfad)

Wenn Sie diese Option auswählen, werden Ihre verschlüsselten Wiederherstellungsdaten z.B. auf einem Server abgelegt. Bei Auswahl dieser Schaltfläche können Sie unter der Option **Am Dateiserver anmelden** Benutzername und Kennwort angeben.

Lokaler Ordner auf Agenten-Computer (nicht empfohlen)

Diese Option ist nur zu empfehlen, wenn Sie die Schlüsseldateien auf einem sicheren Medium (z.B. USB-Gerät) ablegen oder später an einen sicheren Ort verschieben.

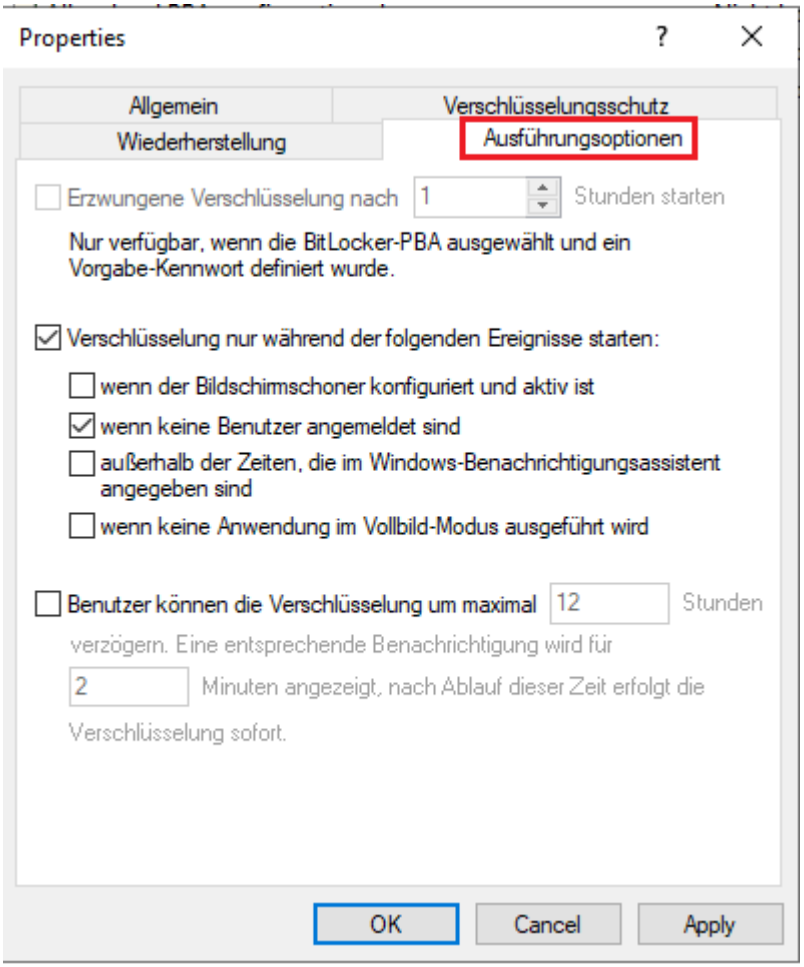
2.2.3.4 Reiter Ausführungsoptionen

Auf diesem Reiter sind Optionen für Start und Verzögerung der Verschlüsselung, sowie für die erzwungene Verschlüsselung wählbar.

Der Start der BitLocker-Verschlüsselung auf den DriveLock Agenten kann zum Einen von bestimmten Ereignissen abhängig gemacht werden oder zum Anderen durch den Benutzer verzögert werden. Ziel ist dabei, den Benutzer möglichst wenig zu stören und die Rechnerleistung konstant zu halten, ohne dabei auf die Sicherheit durch die Verschlüsselung verzichten zu müssen.

Sie können die Option **Erzwungene Verschlüsselung nach x Stunden starten** nur dann auswählen, wenn Sie bei den Einstellungen für die Pre-Boot-Authentifizierung die BitLocker-PBA ausgewählt und ein Kennwort vorgegeben haben. Wenn der Benutzer bis zum Ablauf der vorgegebenen Zeit noch kein eigenes Kennwort vergeben hat, wird eine Verschlüsselung mit dem vorgegebenen Kennwort durchgeführt. Dabei wird vom erstmaligen Anzeigen des Kennwortdialogs gezählt.

Mit der Option **Verschlüsselung nur während der folgenden Ereignisse starten:** geben Sie Bedingungen an, wann die Verschlüsselung starten darf. Wenn Sie beispielsweise festlegen wollen, dass die Verschlüsselung nur dann auf einem Client-Computer durchgeführt wird, wenn keine Benutzer angemeldet sind, setzen sie die Option wie in der Abbildung unten:



Hinweis: Beachten Sie bei der Option **wenn keine Anwendung im Vollbild-Modus ausgeführt wird**, dass die Anwendung tatsächlich im Vollbildmodus und nicht nur maximiert ausgeführt wird. Diese Option ist beispielsweise bei der Ausführung von CAD/CAM-Anwendungen von Bedeutung.

Im unteren Bereich geben Sie die Anzahl der Stunden an, um die Benutzer die Verschlüsselung maximal verzögern dürfen. Als Wert sind hier bis zu 9000 Std. möglich. Außerdem geben Sie an, wie lange die Verzögerungsbenachrichtigung beim Benutzer angezeigt wird. Sobald diese Zeit abgelaufen ist und der Benutzer keinerlei Aktion an seinem Client-Computer durchgeführt hat, startet die Verschlüsselung automatisch. Gleiches gilt, wenn kein Benutzer angemeldet ist.

Hinweis: Sobald die Verzögerungsbenachrichtigung beim Benutzer erscheint, wird die Verschlüsselung gestartet und die Protektoren werden bereits angelegt. Unmittelbar danach wird die Verschlüsselung angehalten, um dann wieder fortgesetzt zu werden, sobald der Benutzer in der Benachrichtigung auf Verschlüsseln klickt oder die Verzögerungszeit ausläuft (ohne Benutzerinteraktion). Dann wird weiter ver-

schlüsselt. Das System ist zu dem Zeitpunkt bereits sicher und der Benutzer muss bei einem Neustart schon ein Kennwort (oder den PIN bei TPM) angeben.

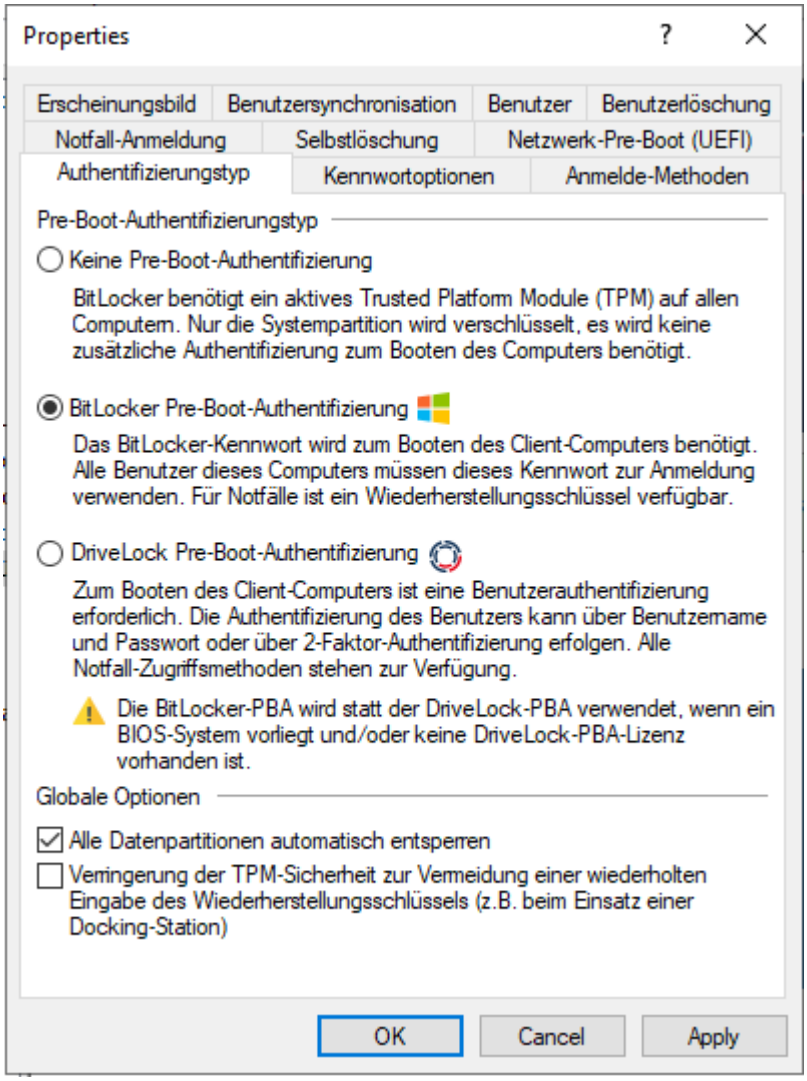
2.2.4 Einstellungen für die Pre-Boot-Authentifizierung

2.2.4.1 Authentifizierungstyp

Die Wahl des Pre-Boot-Authentifizierungstyps (PBA) hängt davon ab, ob die Computer, deren Festplatten Sie verschlüsseln wollen, ein TPM (Trusted Platform Module) enthalten oder nicht.

Im Beispiel unten soll explizit die BitLocker Pre-Boot-Authentifizierung verwendet werden. Informationen zur DriveLock Pre-Boot-Authentifizierung für BitLocker erhalten Sie im entsprechenden Kapitel.

Folgende Optionen stehen auf dem Reiter **Authentifizierungstyp** zur Verfügung:



1. Wählen Sie die erste Option **Keine Pre-Boot-Authentifizierung**,
   - wenn auf den zu verschlüsselnden Festplatten ein TPM vorhanden ist. Dann erübrigt sich eine zusätzliche Authentifizierung beim Starten des Computers.

> Hinweis: Der Protektor, der in diesem Fall angewendet wird, wird als **TPM-Protektor** bezeichnet.

- Beim Verschlüsseln greift BitLocker hier auf ein TPM zu, das zuvor im BIOS aktiviert werden muss.
- Eine Kennwortvergabe ist in diesem Fall nicht notwendig, Sie können Ihre Auswahl speichern und den Dialog schließen.

2. Wählen Sie die zweite Option **BitLocker Pre-Boot-Authentifizierung** (s. Abbildung),
   - wenn auf den zu verschlüsselnden Festplatten kein TPM vorhanden ist oder Sie sich nicht sicher sind, ob ein TPM aktiviert ist.
   - In diesem Fall wird die original Windows BitLocker PBA verwendet.
   - Öffnen Sie den Reiter **Kennwortoptionen**, um ein Kennwort zu vergeben oder eine der anderen Optionen auszuwählen.

> Hinweis: Die Optionen auf diesem Reiter stehen nur zur Verfügung, wenn Sie **BitLocker Pre-Boot-Authentifizierung** als **Authentifizierungstyp** gewählt haben.
> Die anderen Reiter sind inaktiv, da sich die entsprechenden Optionen ausschließlich auf den Authentifizierungstyp **DriveLock Pre-Boot-Authentifizierung** beziehen.

3. Wir empfehlen bei beiden Möglichkeiten ein Häkchen bei der Option **Alle Datenpartitionen automatisch entsperren** zu setzen, damit bei der Authentifizierung nicht nur die Systempartition entsperrt wird, sondern auch die Datenpartitionen der Computer, denen diese Richtlinie zugewiesen wird.

> Hinweis: Im Gegensatz zu Microsoft entsperrt DriveLock die Datenpartitionen automatisch für alle Benutzer eines Computers. Der Entsperrvorgang durch DriveLock BitLocker Management geschieht unabhängig von der Windows Bitlocker Funktion, was zur Folge hat, das der Aufruf `manage-bde -status` bei durch DriveLock entsperrten Laufwerken immer noch "Automatic Unlock: Disabled" zurückgibt.

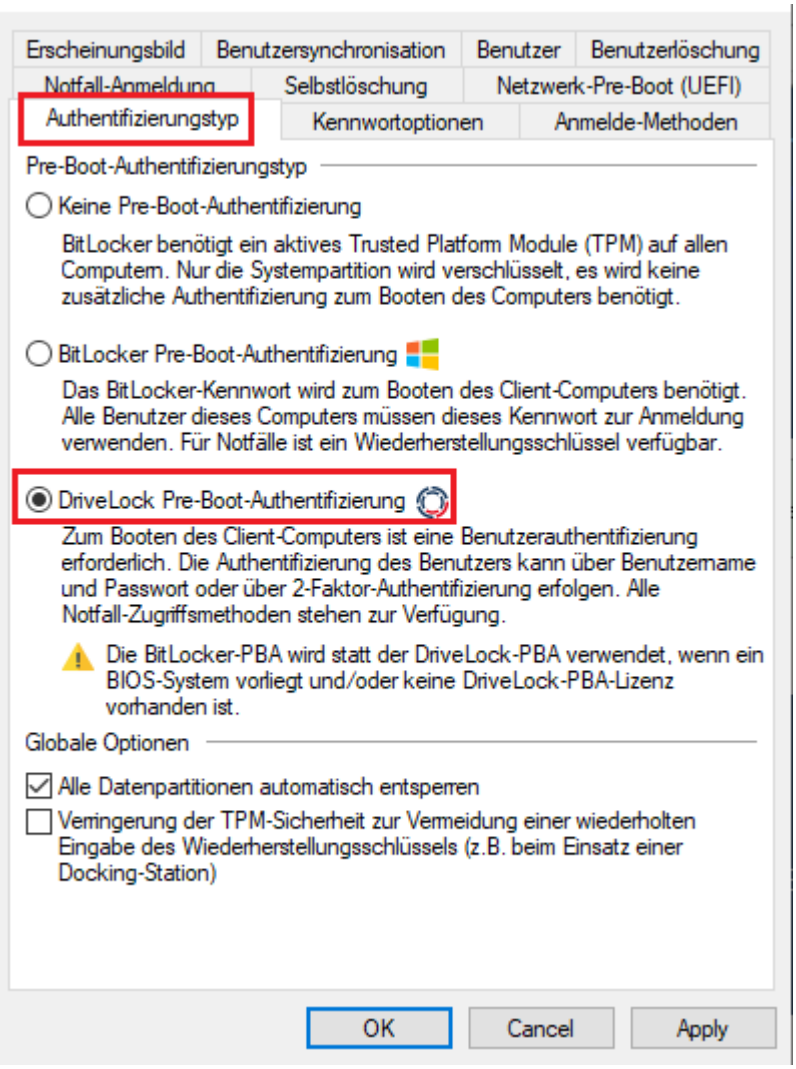
4. Mit der Option **Verringerung der TPM-Sicherheit ...** kann die TPM-Plattformvalidierung angepasst werden. Die Option ist beispielsweise sinnvoll, wenn bei BitLocker-verschlüsselten Laptops der Wiederherstellungsschlüssel immer wieder angefordert wird, sobald der Laptop nicht mit der Dockingstation verbunden ist. Die neue Option wirkt sich auf jeden Pre-Boot-Authentifizierungstyp aus, da DriveLock

TPM-basierte Schutzmechanismen verwendet, sobald TPM verfügbar ist (nur TPM, TPM/PIN, TPM/StartupKey). Die Option ist standardmäßig deaktiviert.

2.2.4.1.1 Option: DriveLock Pre-Boot-Authentifizierung

Öffnen Sie die **Einstellungen für die Pre-Boot-Authentifizierung** und wählen Sie zunächst auf dem Reiter **Authentifizierungstyp** die Option **DriveLock Pre-Boot-Authentifizierung**.

Hinweis: Wenn diese Option nicht wählbar ist, überprüfen Sie, dass die DriveLock PBA Option korrekt lizenziert ist und dass Sie die Richtlinie nach Aktivierung der Lizenzoption gespeichert und neu geöffnet haben.



Achtung: Diese Option ist nur für Computer mit dem Betriebssystem Windows 10 und höher und UEFI-Firmware verfügbar. Server- und ältere Systeme sowie Systeme mit Legacy BIOS werden nicht unterstützt.

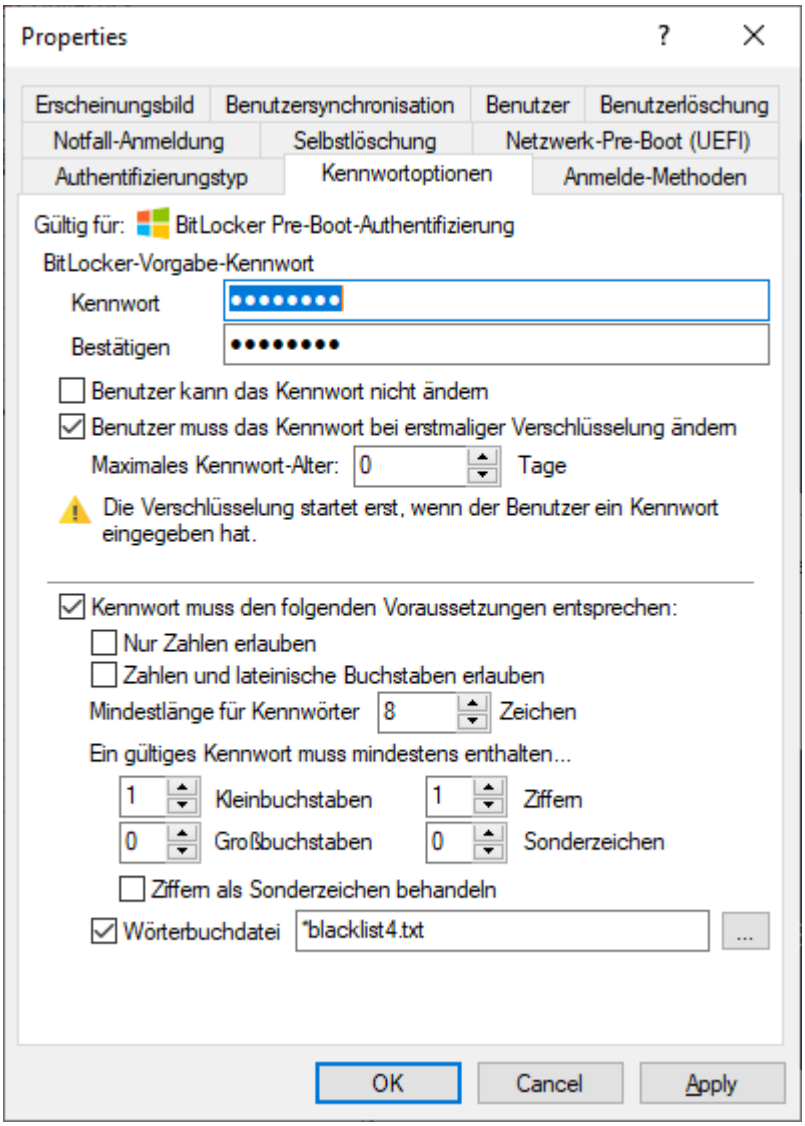
Bitte beachten Sie außerdem:

- Wenn die Voraussetzungen auf dem Client-Computer nicht gegeben sind, wird automatisch die Option **BitLocker Pre-Boot-Authentifizierung** verwendet.
- Für die DriveLock Pre-Boot-Authentifizierung hat die Option **Alle Datenpartitionen automatisch entsperren** keine Auswirkung, weil Datenlaufwerke generell automatisch entsperrt werden.

Auf dem Reiter **Kennwortoptionen** sind keine Angaben möglich. Wenn Sie auf diesem Reiter Anpassungen vornehmen wollen, (z.B. für Computer, auf denen DriveLock Pre-Boot-Authentifizierung nicht verwendet werden kann), muss vorübergehend die Option **BitLocker Pre-Boot-Authentifizierung** aktiviert werden.

2.2.4.2 Kennwortoptionen

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



Achtung: Bitte beachten Sie, dass sich diese Kennworteinstellung nur auf den Endbenutzer bezieht.

1. Sie geben ein **BitLocker-Kennwort** an und wählen sonst keine der anderen Möglichkeiten im oberen Dialogbereich aus:
   - Die Verschlüsselung startet sobald sie aktiviert bzw. die Richtlinie zugewiesen ist. Der Benutzer am Client-Computer kann das Kennwort nachträglich ändern oder das von Ihnen vorgegebene Kennwort weiterverwenden.

     Hinweis: Bitte beachten Sie, dass es in Ihrer Verantwortung liegt, dem Benutzer das Kennwort über einen sicheren Kanal mitzuteilen.

2. Sie setzen ein Häkchen bei der Option **Benutzer kann Kennwort nicht ändern**:

- Sie legen ein BitLocker-Kennwort fest, das der Benutzer nie ändern kann. Die Initial-Verschlüsselung startet automatisch, auch ohne Anmeldung des Benutzers am Client-Computer, nachdem Sie die Verschlüsselung aktivieren bzw. die Richtlinie zugewiesen haben.
- Sobald ein Benutzer den Computer startet, muss dieses BitLocker-Kennwort eingegeben werden, um die verschlüsselten Festplatten zu entsperren.

> Hinweis: Bitte teilen Sie dem Benutzer das Kennwort über einen sicheren Kanal mit.

- Die Eingabe des Kennworts erfolgt unabhängig vom Verschlüsselungsfortschritt, d.h. sobald die Verschlüsselung gestartet ist, muss das BitLocker-Kennwort in der PBA eingegeben werden.

3. Sie setzen ein Häkchen bei der Option **Benutzer muss Kennwort bei erstmaliger Verschlüsselung ändern** (s. Abbildung):
   - Sie geben kein BitLocker-Kennwort vor und überlassen es dem Benutzer, selbst ein Kennwort festzulegen.
   - Die Komplexitätsvoraussetzungen können Sie vorgeben.
   - Die Verschlüsselung startet, sobald der Benutzer das BitLocker-Kennwort festgelegt hat.
   - Das Kennwort kann nachträglich geändert werden.
   - Mit der Einstellung **Maximales Kennwort-Alter** geben Sie die Anzahl der Tage an, nach denen der Endbenutzer das Kennwort erneut ändern muss.

Mit den Optionen unterhalb von **Kennwort muss den folgenden Voraussetzungen entsprechen:** geben Sie genaue Kriterien vor, denen ein vom Benutzer vergebenes Kennwort entsprechen muss. Die Option ist standardmäßig ausgewählt.

1. Die Option **Nur Zahlen erlauben** kann in dem Fall ausgewählt werden, wenn alle Client-Computer über ein TPM verfügen und somit 6 Zeichen erlaubt sind.

> Achtung: Wenn auf Client-Computern kein TPM vorhanden ist oder Nicht-Systempartitionen mit verschlüsselt werden müssen, ist die Vorgabe weiterhin mindestens 8 Zeichen. (Vorgabe von Microsoft für Passwörter auf Datenpartitionen).

2. Die Option **Zahlen und lateinische Buchstaben erlauben** schränkt die Verwendung der gültigen Zeichen ein. Sonderzeichen können mit dieser Einstellung nicht mehr verwendet werden. Beachten Sie dabei den Hinweis im Kapitel Anmeldung an BitLocker.
3. Unter **Ein gültiges Kennwort muss mindestens enthalten...** definieren Sie die Anzahl der Buchstaben, Zahlen und Sonderzeichen:
   - Die Kennwortlänge muss zwischen 8 und 20 Zeichen sein. Eine Anzahl unter 8 oder über 20 führt zu einer Fehlermeldung.
   - Definieren Sie weitere Mindestanforderungen (Anzahl der Buchstaben, Sonderzeichen usw.) je nach Ihren Vorstellungen.
   - Wenn Sie die Option **Ziffern als Sonderzeichen behandeln** aktivieren, gelten Ziffern sowohl als Ziffern, als auch als Sonderzeichen. Achten Sie deshalb bei der Angabe der Ziffern und Sonderzeichen auf Übereinstimmung.
4. Mit der Option **Wörterbuchdatei** können Sie ein Wörterbuch auswählen, in dem Sie Kennwörter festgelegt haben, die nicht verwendet werden dürfen. Die Wörterbuchdatei muss zuvor im Dateispeicher angelegt worden sein. Bei der Kennwortvergabe wird diese Datei dann überprüft und das Kennwort entsprechend zugelassen oder abgelehnt.
   In der Abbildung oben wird die Datei *blacklist4.txt als Wörterbuchdatei verwendet.

> Hinweis: Beachten Sie, dass auch Kennwörter verweigert werden, in denen auch nur ein Teil des Kennwortes im Wörterbuch vorkommt (z.B.: wenn das Wörterbuch „es“ enthält, werden Kennwörter wie „Essen“, „vergessen“ oder „Sessel“ nicht erlaubt).

2.2.4.3 Anmelde-Methoden

Auf diesem Reiter haben Sie folgende Möglichkeiten:

Wählen Sie die Option **Single Sign-on für Windows**, damit nur eine einzige Anmeldung am Client-Computer notwendig ist. Die Windows Anmeldemaske erscheint dann nicht mehr.

Folgende Authentifizierungsmethoden stehen zur Auswahl:

- **Lokale Anmeldung**: Diese Option ist standardmäßig aktiviert. Diese Methode erlaubt es lokalen Windows-Benutzern, sich mit ihrem lokalen Windows Benutzernamen, Kennwort und lokalen Systemnamen am System zu authentifizieren.

- **Domänenbenutzer (mit Kennwort)**: Diese Methode erlaubt es Windows Domänen-Benutzern sich mit ihrem Windows Domänen-Benutzernamen, Kennwort und Domänennamen am System zu authentifizieren.

  Achtung: Nur wenn die Optionen Windows und Pre-Boot gesetzt sind, können sich Benutzer überhaupt an der Domäne anmelden.

- **Domänenbenutzer (mit Token)**: Diese Methode erlaubt es Windows Domänen-Benutzern, eine Smartcard/Token und PIN für die Authentifizierung zu benutzen.

Anmeldung mit Kennwort-Token erlauben: Diese Methode erlaubt die Pre-Boot Authentifizierung für einen Kennwort-Token Benutzer. Wenn diese Option markiert ist, muss mindestens noch eine Windows Authentifizierung ausgewählt werden.

Achtung: Bevor Sie die DriveLock-PBA nur für Token-Zugriff konfigurieren, müssen Sie sicherstellen, dass es ein gültiges Token sowohl für die PBA als auch für die Windows-Anmeldung (Entsperren) existiert.

Weitere Optionen im Dialog:

- Die Option **Maximale Anzahl Anmeldungen vor Sperre** führt dazu, dass nach der festgelegten Anzahl von fehlerhaften Anmeldungen ein Benutzer für eine bestimmte Zeit gesperrt werden kann, um das System vor einer Brute-Force Attacke mit automatischen Anmelde-Skripten zu schützen. Ändern Sie die Standard-Werte gemäß Ihren Unternehmens-Sicherheitsrichtlinien.
- Wenn Sie Zertifikate für die Authentifizierung benutzen, können Sie die Anzahl der Tage festlegen, nach denen DriveLock die Benutzer vor Ablauf der Zertifikate warnt.
- Die Option **Anmeldungen global für alle Benutzer zählen** ist standardmäßig aktiviert. Sie bewirkt, dass Fehlversuche nicht für einen einzelnen Benutzer hochgezählt werden, sondern der Zähler für Fehlversuche unabhängig vom verwendeten Benutzer inkrementiert wird.
- Mit der Option **Pre-Boot-Authentifizierung bis zur ersten Windows-Anmeldung deaktivieren** wird die PBA so lange deaktiviert, bis sich der erste Benutzer an Windows angemeldet hat. Damit wird verhindert, dass sich nur die Benutzer anmelden können, deren Namen auf dem Reiter Benutzer unter Pre-Boot-Authentifizierungsbenutzer eingetragen wurden. Ohne vorherige gültige Windows-Anmeldung werden also die in der Richtlinie angegebenen Benutzer ignoriert.

2.2.4.4 Erscheinungsbild

Legen Sie auf diesem Reiter fest, wie die DriveLock-PBA bei Benutzern auf ihren Client-Computern angezeigt wird.

- Als **Hintergrundbild** stehen verschiedenen Vorlagen zur Auswahl. Wählen Sie eine davon aus.
- Sie können auch Ihr eigenes Hintergrundbild wählen, indem Sie ein **benutzerspezifisches** aus dem Dateisystem oder dem Richtliniendateispeicher auswählen.
- Mit der Option **Kennwort anzeigen** kann der Benutzer kurz das eingegebene Kennwort im Klartext anzeigen lassen.
- Falls gewünscht, können Sie Ihren eigenen Anzeigetext im Textfeld unter der Option **Pre-Boot-Benutzerinformationen anzeigen**eingeben.

2.3 Entschlüsselung

Die Entschlüsselung wird mit einer einzigen Einstellung angestoßen, die in den **Einstellungen für die Verschlüsselung** auf dem Reiter **Allgemein** gesetzt wird.

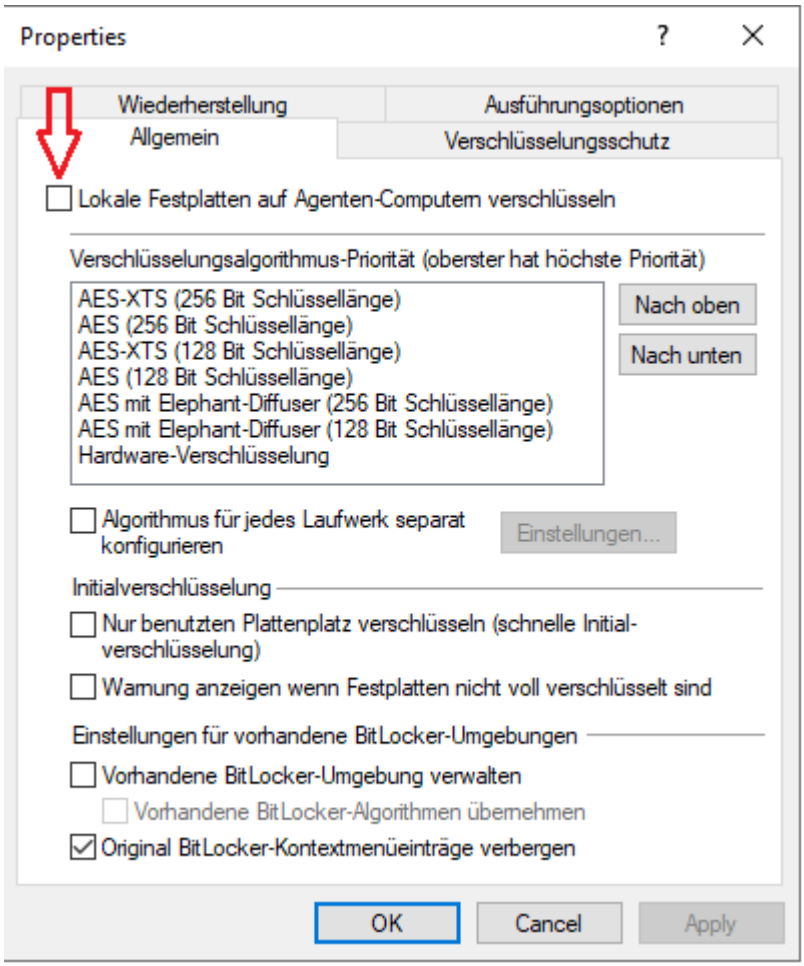
Der Entschlüsselungsprozess lässt sich, ebenso wie der Verschlüsselungsprozess, auch im DriveLock Operations Center (DOC) nachverfolgen.

Im Ereignisreport (BitLocker Ereignisse) wird ebenfalls Information über die Entschlüsselung einzelner Computer ausgegeben.

2.3.1 Verschlüsselte Festplatten entschlüsseln

Um die Entschlüsselung bereits verschlüsselter Festplatten anzustoßen, gehen Sie wie folgt vor:

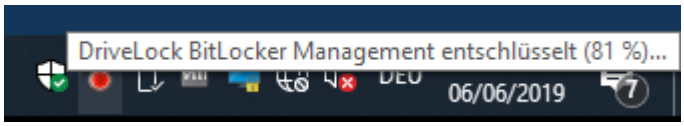
1. Öffnen Sie die entsprechende BitLocker-Richtline.
2. Öffnen Sie den Dialog **Einstellungen für die Verschlüsselung** und hier den Reiter **Allgemein**.
3. Entfernen Sie das Häkchen bei der Option **Lokale Festplatten auf Agenten-Computern verschlüsseln**.



4. Setzen Sie auf dem Reiter **Verschlüsselungsschutz** bei der Einstellung **Entschlüsselung um *x* Tage verzögern** einen Wert ein. Der Standardwert ist **3**, d.h. die Entschlüsselung startet nach 3 Tagen. Je nach Wert wird die Entschlüsselung um x Tage hinausgezögert.

> Hinweis: Wenn Sie die Entschlüsselung sofort starten wollen, müssen Sie hier den Wert **0** eingeben.

5. Die Einstellung **Keine Entschlüsselung durchführen** ist die Standardeinstellung, die eine ungewollte Entschlüsselung verhindern soll. Sie wird deaktiviert, sobald Sie einen Wert für die Verzögerung eingeben.
6. Bestätigen Sie Ihre Einstellungen mit **OK**.
7. Auf dem Computer, dessen Festplatte entschlüsselt wird, erscheint nun folgende Meldung in der Statusleiste:



2.4 Richtline überschreiben (BitLocker)

Um auf einzelnen Client-Computern gezielt Verschlüsselungseinstellungen außer Kraft zusetzen, können Sie die jeweiligen Richtlinieneinstellungen überschreiben.

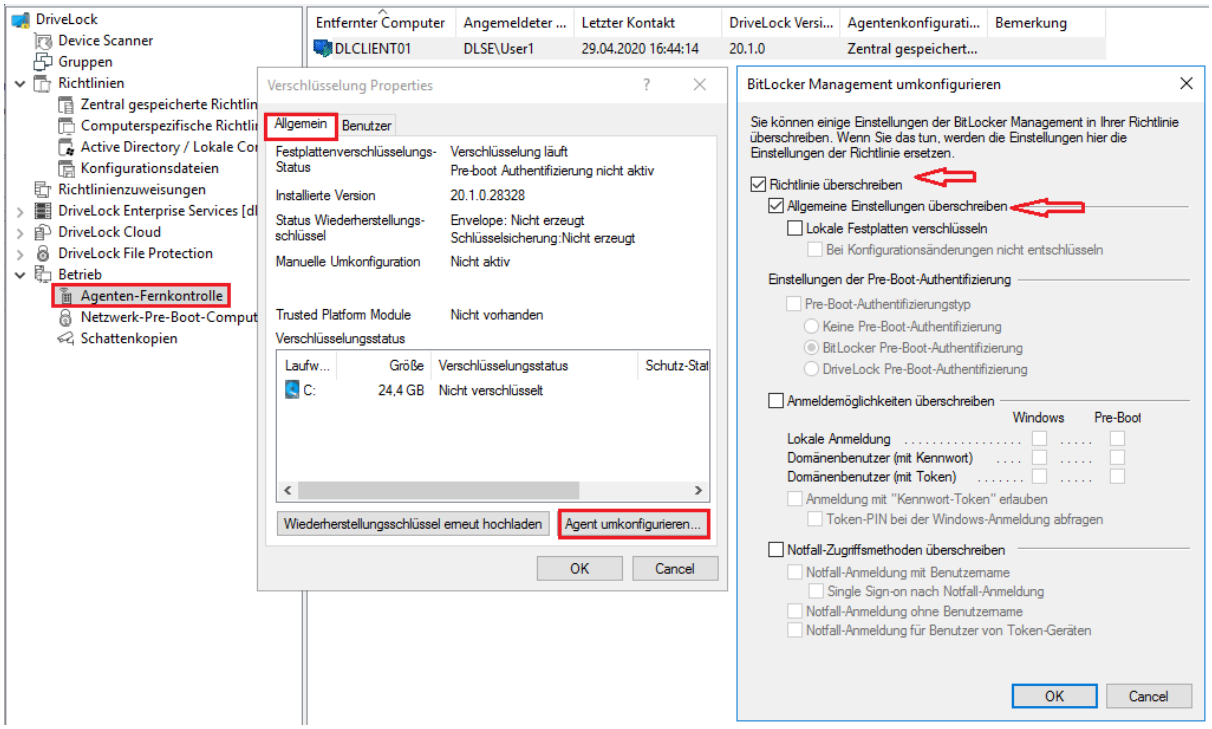
> Achtung: Beachten Sie bitte, dass die Richtlinieneinstellungen erst dann wieder aktiv werden, wenn Sie die Umkonfiguration wieder rückgängig gemacht haben.

Gehen Sie folgendermaßen vor:

1. Öffnen Sie die **Agenten-Fernkontrolle** im Knoten **Betrieb**.
2. Markieren Sie den Client-Computer, dessen Richtlinie Sie überschreiben wollen.
3. Wählen Sie aus dem Kontextmenü den Menüpunkt **Verschlüsselungs-Eigenschaften...**.

   > Hinweis: Beachten Sie bitte, dass eine Verbindung zwischen DES und DriveLock Agenten bestehen muss, damit die Verschlüsselungs-Eigenschaften angezeigt werden können.

4. Auf dem Reiter **Allgemein** sehen Sie Informationen zur Verschlüsselung des DriveLock Agenten. Klicken Sie auf die Schaltfläche **Agent umkonfigurieren...**.
5. Wenn Sie die Option **Richtlinie überschreiben** auswählen und die Option **Allgemeine Einstellungen überschreiben** gesetzt lassen (Standardeinstellung), wird der DriveLock Agent sofort entschlüsselt und BitLocker deaktiviert (siehe Abbildung).



6. Durch Setzen der Option **Lokale Festplatten verschlüsseln** werden die Verschlüsselungseinstellungen aus der Richtlinie (z.B. Algorithmus oder Schnellverschlüsselung) übernommen.
7. Wenn Sie die Option **Bei Konfigurationsänderungen nicht entschlüsseln** wird die entsprechende Richtlinienoption (Keine Entschlüsselung durchführen) überschrieben.
8. Wenn Sie jetzt **OK** klicken, werden Ihre Einstellungen mit sofortiger Wirkung auf dem gewählten Client-Computer angewendet.

2.5 Beispielkonfiguration

Im folgenden finden Sie eine Beispielkonfiguration für die Verschlüsselung mit erforderlicher Kennworteingabe durch den Benutzer am Client-Computer.

Führen Sie die folgenden Anweisungen in der angegebenen Reihenfolge durch, um eine schnelle und unkomplizierte Verschlüsselung der Festplatten auf Ihren Client-Computern zu erreichen.

Dieser Beispielprozess beginnt bei der Lizenzierung von DriveLock BitLocker Management und endet bei der Verschlüsselung der Festplatten auf den Client-Computern.

> Hinweis: Weiterführende Informationen zu den jeweiligen Arbeitsschritten finden Sie unter den Verweisen.

1. Legen Sie eine neue Richtlinie an oder verwenden Sie eine bereits angelegte.
   In dieser Dokumentation wird die Richtlinie als 'BitLocker-Richtlinie' bezeichnet.
2. Tragen Sie die entsprechenden Lizenzen in der Richtlinie ein und lizenzieren Sie alle Computer.
3. Öffnen Sie in der Richtlinie den Knoten **Verschlüsselung** und wählen Sie im Unterknoten **BitLocker Management** den Menüpunkt **Festplatten-Verschlüsselung**.
   Mehr dazu hier.
4. Erstellen Sie zunächst die Verschlüsselungszertifikate.
5. Öffnen Sie die Einstellungen für die Installation und geben Sie an, welche Benachrichtigungen ein Benutzer am Client-Computer angezeigt bekommen soll.
6. Anschließend setzen Sie die Einstellungen für die Pre-Boot-Authentifizierung:
   - Wählen Sie auf dem Reiter **Authentifizierungstyp** die Option **BitLocker Pre-Boot-Authentifizierung**.
     Setzen Sie ein Häkchen bei **Alle Datenpartitionen automatisch entsperren**.
   - Auf dem Reiter **Kennwortoptionen** wählen Sie die Option **Benutzer muss Kennwort ändern** und geben die von Ihnen gewünschten Komplexitätsvorgaben für das Kennwort an.

   Klicken Sie **Bestätigen**, um Ihre Eingaben zu übernehmen und schließen Sie den Dialog mit **OK**.
7. In den Einstellungen für die Verschlüsselung geben Sie folgendes vor:

- Öffnen Sie den Reiter **Allgemein**.
  1. Als erstes setzen Sie ein Häkchen bei der Option **Lokale Festplatten auf Agenten-Computern verschlüsseln**.
  2. Dann setzen Sie den Eintrag **AES-XTS (256 Bit Schlüssellänge)** an die höchste Stelle in der Verschlüsselungsalgorithmus-Priorität.
  3. Setzen Sie optional ein Häkchen bei **Einstellung pro Laufwerk konfigurieren** und wählen dort für die Laufwerke C: und die voraussichtlichen Datenlaufwerke über die Schaltfläche **Ändern** den oben genannten Verschlüsselungsalgorithmus. Sie können auch **Nicht verschlüsselt** angeben, wenn keine Verschlüsselung gewünscht ist.
  4. Schließen Sie den Dialog mit **OK**.
  5. Wählen Sie unter Initialverschlüsselung die Option **Nur benutzten Plattenplatz verschlüsseln (schnelle Initialverschl.)** und korrigieren Sie unter Installations-Schutz die Anzahl der Tage bei der Entschlüsselungs-Verzögerung auf '**0**'.
- Öffnen Sie jetzt den Reiter **Wiederherstellung** und wählen Sie die erste Option **DriveLock Enterprise Service**.

Schließen Sie den Dialog mit **OK**.

8. Speichern und veröffentlichen Sie die Richtlinie.
9. Ihre Einstellungen werden bei der nächsten Konfigurationsaktualisierung des Client-Computers aktiviert.
10. Die Festplattenverschlüsselung auf den Client-Computern wird je nach Einstellung sofort oder nach Eingabe des Kennworts seitens des jeweiligen Benutzers ausgeführt.
11. Hinweis: Weitere Informationen zur Installation des Agenten oder zur Richtlinienerstellung finden Sie in den Dokumentationen zur DriveLock Installation und Administration unter https://drivelock.help/.

2.6 Wiederherstellung

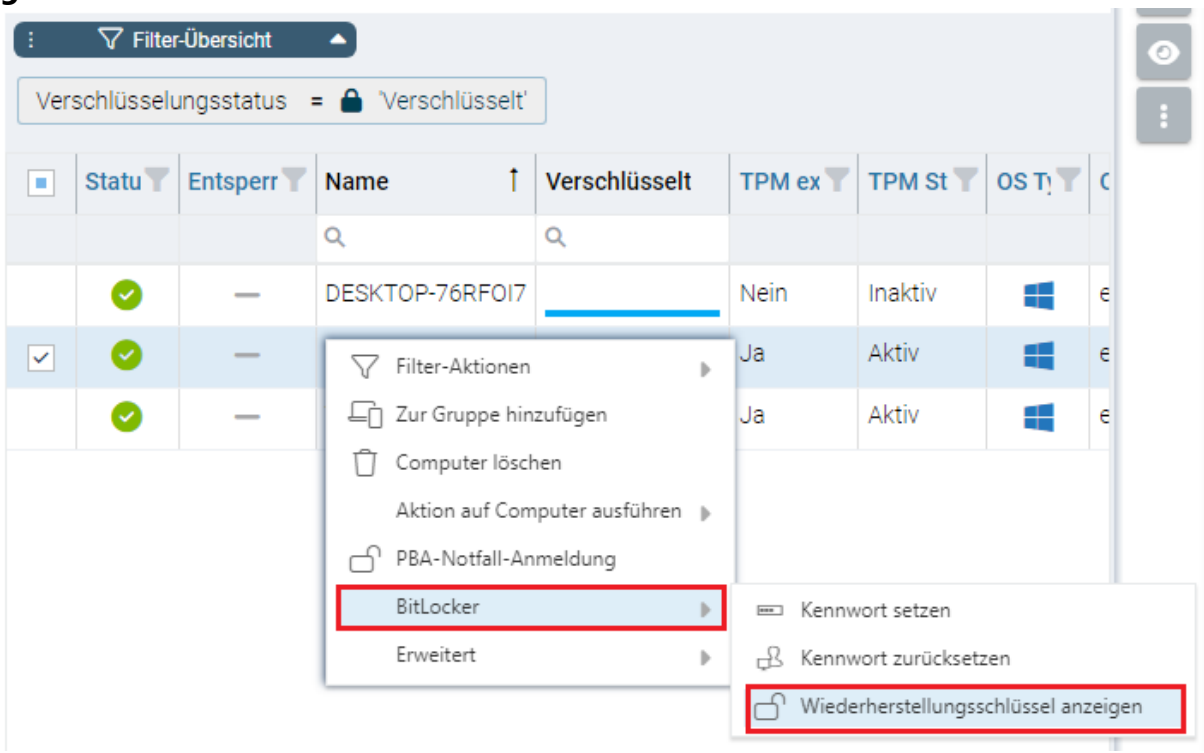
2.6.1 Wiederherstellung verschlüsselter Festplatten

Wenn ein Benutzer nicht mehr auf seine mit BitLocker Management verschlüsselte Festplatte (Systempartition) zugreifen kann, weil er beispielsweise sein BitLocker-Kennwort vergessen hat, muss der Zugriff durch Verwendung des Wiederherstellungszertifikats und des dazugehörigen privaten Schlüssels ermöglicht werden.

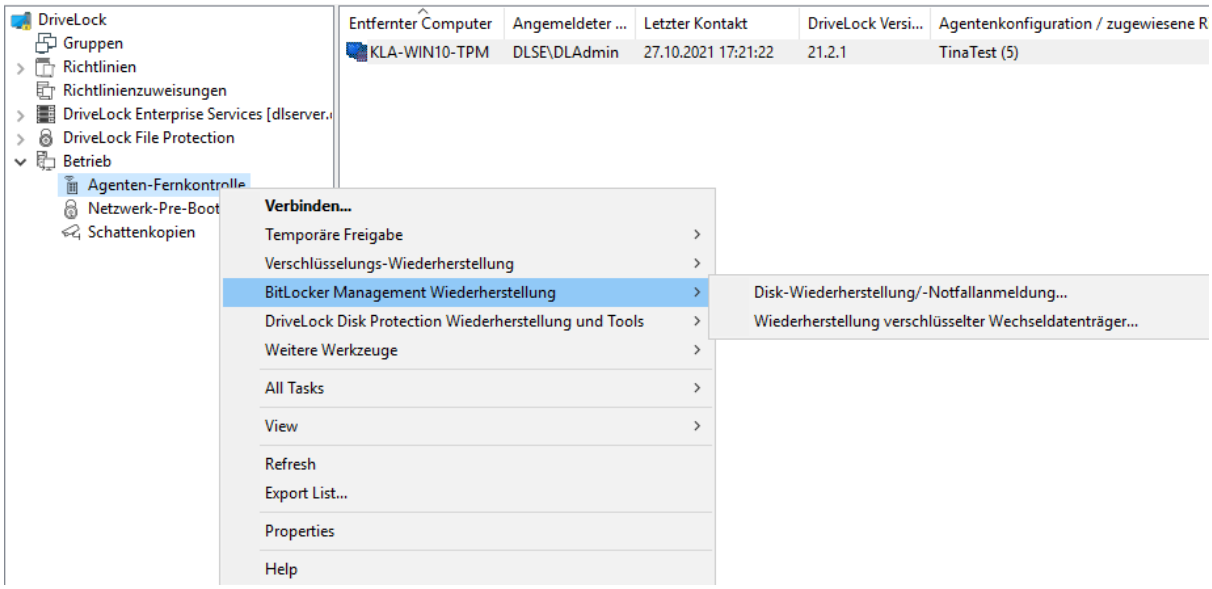
Hinweis: Das Hochladen der Wiederherstellungsdaten geschieht dann, wenn alle zur Verschlüsselung notwendigen Laufwerke mit der Verschlüsselung begonnen haben.

In diesem Fall müssen Sie den Wiederherstellungsprozess starten. Dazu bietet Ihnen DriveLock zwei Möglichkeiten an:

1. Für den Wiederherstellungsprozess im **DriveLock Operations Center** wählen Sie den entsprechende Rechner über die Ansicht **Computer** aus. Öffnen Sie das Kontextmenü und wählen das Untermenü **BitLocker** und dann **Wiederherstellungsschlüssel anzeigen**.



2. Für den Wiederherstellungsprozess in der **DriveLock Management Konsole** wählen Sie den Knoten **Betrieb**, öffnen dann das Kontextmenü der **Agenten-Fernkontrolle** und wählen dann den Menüpunkt **BitLocker Wiederherstellung** (s. Abbildung).



Hier öffnet sich der Wiederherstellungsassistent, der Sie durch die jeweiligen Schritte führt.

2.6.1.1 Entsperren von BitLocker-verschlüsselten Datenpartitionen

Datenpartitionen, die zuvor in anderen Computern verwendet und auch mit DriveLock verwaltet wurden, können nicht automatisch entsperrt werden. Sie haben zwei Möglichkeiten, diese über den Kommandozeilenparameter `blunlockdatadrives` zu entsperren: entweder mithilfe eines API-Schlüssels oder über die Eingabe von Benutzername und Kennwort.

- Bei der Eingabe von Benutzernamen und Kennwort lautet die Aufrufsyntax:

```
DriveLock -blunlockdatadrives -user:JohnDoe@company.com -pass-
word:"mypassword &%"
```

Der Benutzer, in diesem Beispiel "JohnDoe" muss über entsprechende Berechtigungen verfügen, die im DriveLock Operations Center unter Berechtigungen/ Rollenzuweisungen einzustellen sind. Die Rolle **Wiederherstellungsschlüssel anzeigen** muss dabei zugewiesen sein.

- Die Syntax bei Verwendung eines API-Schlüssels lautet:

```
DriveLock -blunlockdatadrives -pass-
word:"Ac-
nefi6C+mxjDM/1AZb76vH9-
zuh17WFd2EnigJODrDDdA+Sy3V3V512kPKWWivrhMA=="
```

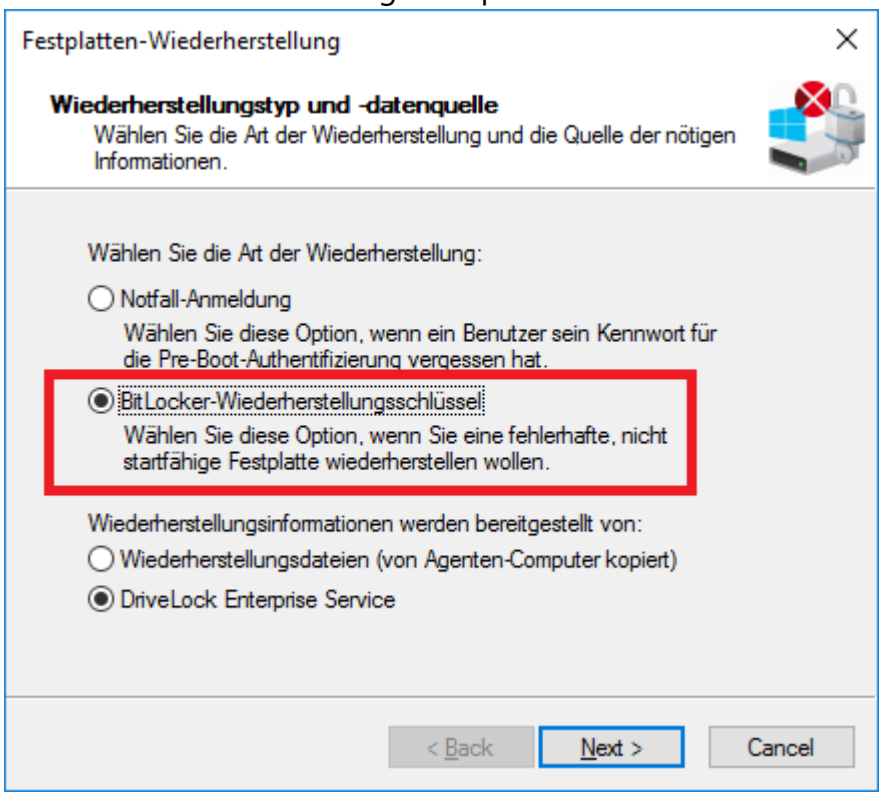
Als Beispiel wurde folgender API-Schlüssel im DOC erzeugt: `Acne-fi6C+mxjDM/1AZb76vH9zuh17WFd2EnigJODrDDdA+Sy3V3V512kPKWWivrhMA==`. Dieser kann jetzt als Ersatz für Benutzername/Kennwort verwendet werden.

Weitere Informationen zum Anlegen eines API-Schlüssels finden Sie in der Admin-Dokumentation.

2.6.2 Vorgehensweise im Richtlinien-Editor

Um den Zugriff auf eine verschlüsselte Festplatte wiederherzustellen, Gehen Sie folgendermaßen vor:

1. Öffnen Sie den Wiederherstellungsassistenten (entweder über das DriveLock Operations Center oder die DriveLock Management Konsole).
2. Wählen Sie im ersten Dialog die Option **BitLocker-Wiederherstellungsschlüssel**.

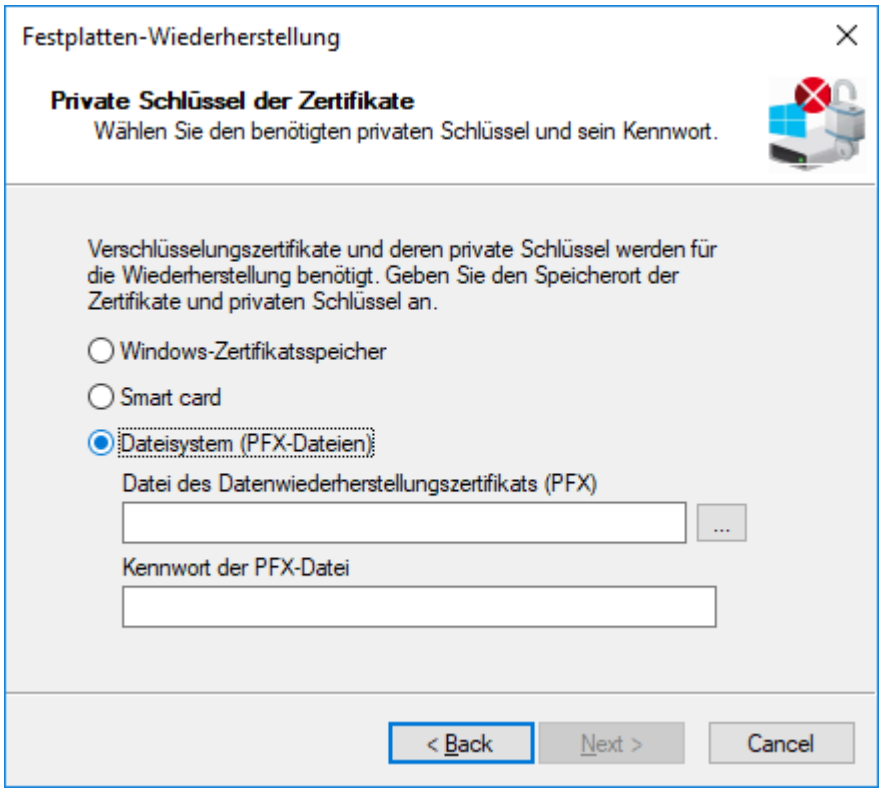


> Hinweis: Informationen zur **Notfall-Anmeldung** an der DriveLock PBA finden Sie im entsprechenden Kapitel.

Wählen Sie weiter unten im Dialog aus, wo sich die **Wiederherstellungsinformationen** befinden.

> Hinweis: Welche Option Sie hier wählen, hängt von Ihren bereits gesetzten Einstellungen zur Verschlüsselung ab. Wir empfehlen die Option DriveLock Enterprise Service.

3. Im folgenden Dialog wählen Sie den exakten Ablageort des Zertifikats bzw. des privaten Schlüssels (*.PFX-Datei) aus.

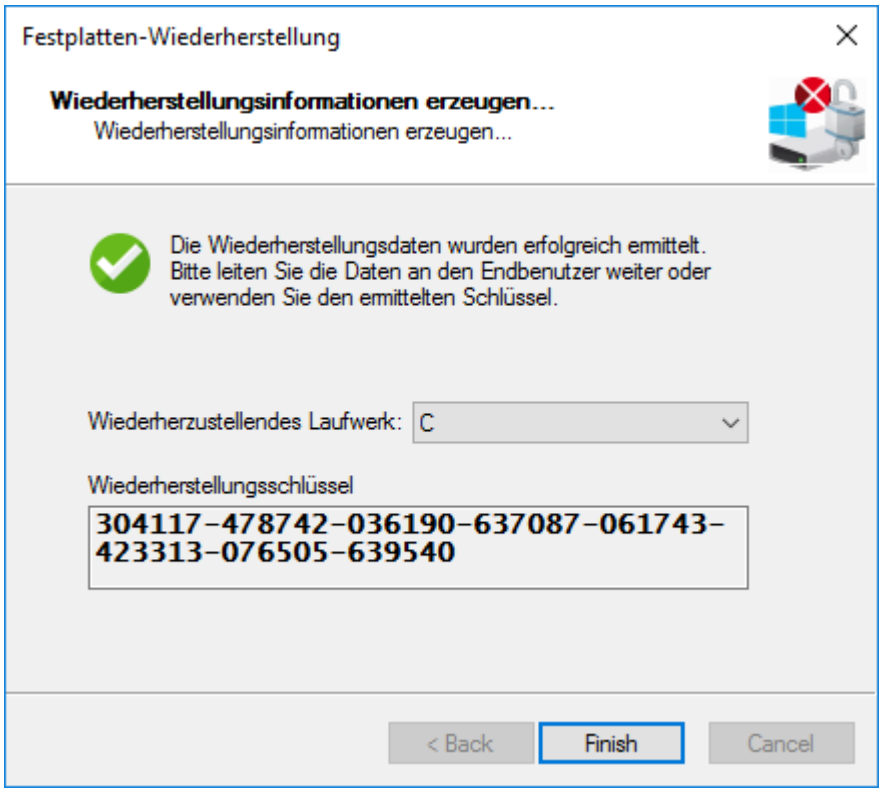


Hier haben Sie auch die Möglichkeit, auf den **Windows Zertifikatsspeicher** zuzugreifen.

> Hinweis: Wenn Sie in den Einstellungen zur Verschlüsselung angegeben haben, dass die Wiederherstellungsinformationen im Dateisystem liegen, müssen Sie hier auch direkt das dazugehörige Kennwort für den privaten Schlüssel eingeben.

4. Wählen Sie als nächstes den Client-Computer aus, dessen Benutzer eine Wiederherstellung angefragt hat. Sie können hier auch nach Computernamen filtern.
5. Fordern Sie im nächsten Dialog den Wiederherstellungsschlüssel an.
6. Warten Sie nun einen Moment ab, während die Wiederherstellungsinformationen ermittelt werden.
7. Der nächste Dialog zeigt Ihnen bereits den Wiederherstellungsschlüssel an.

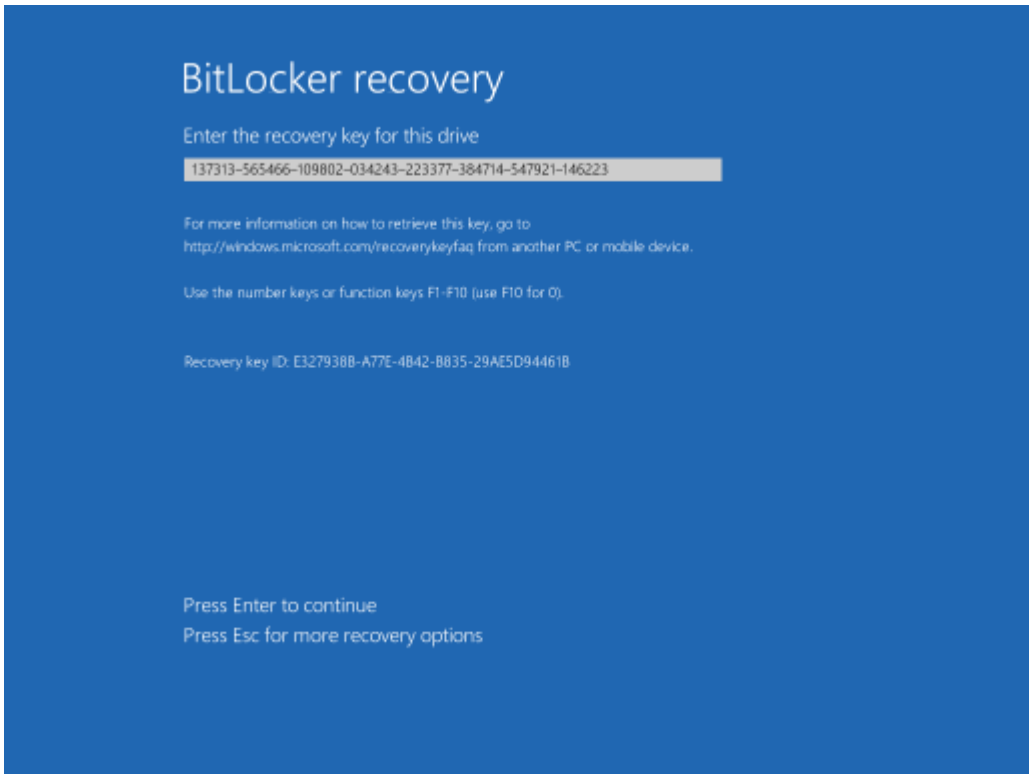
> Hinweis: Wählen Sie hier das Laufwerk aus, das als Systempartition auf dem Client-Computer definiert ist.



8. Teilen Sie nun dem Benutzer den Wiederherstellungsschlüssel mit.

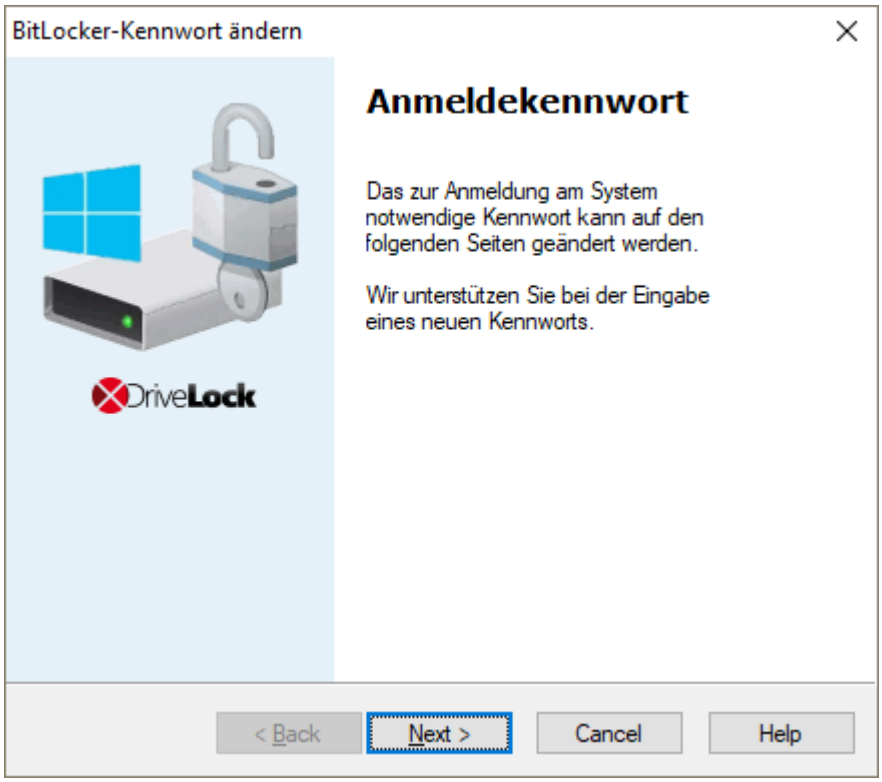
> Hinweis: Bitte beachten Sie, dass es in Ihrer Verantwortung liegt, dem Benutzer den Wiederherstellungsschlüssel über einen sicheren Kanal mitzuteilen.

9. Der Benutzer gibt diesen Schlüssel beim Starten seines Client-Computers in den Dialog **BitLocker recovery** ein.



Hinweis: Bitte beachten Sie, dass dieser Wiederherstellungschlüssel ein erhebliches Sicherheitsrisiko darstellt. Aus diesem Grund veranlasst BitLocker Management eine benutzerseitige Kennwortänderung und tauscht den Wiederherstellungschlüssel gegen einen neuen aus.

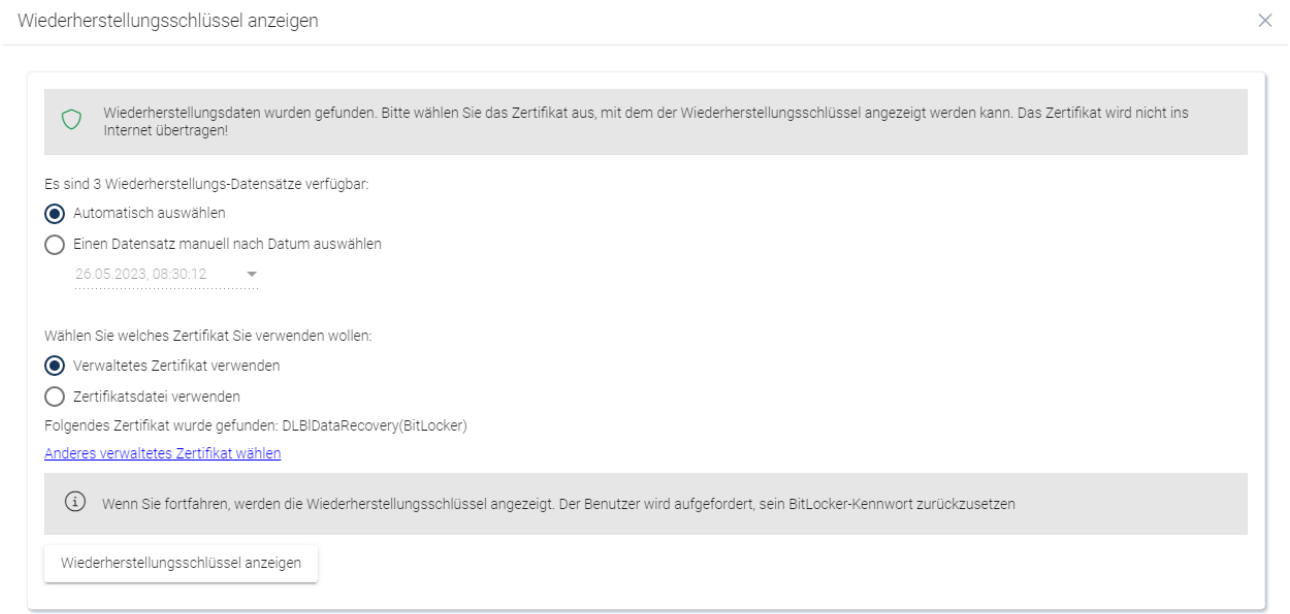
10. Der Assistent zur Änderung des BitLocker-Kennworts startet auf dem Client-Computer und der Benutzer muss ein neues Kennwort erstellen.



11. Sobald das neue Kennwort erstellt ist, kann der Benutzer dieses beim Start des Client-Computers verwenden.

2.6.3 Vorgehensweise im DOC

Sofern Wiederherstellungsdaten vorhanden sind, wird ein Assistent geöffnet, in dem Sie zunächst das Zertifikat bzw. die Zertifikatsdatei auswählen. Falls mehrere Datensätze verfügbar sind, können Sie hier auch den entsprechenden nach Datum auswählen.



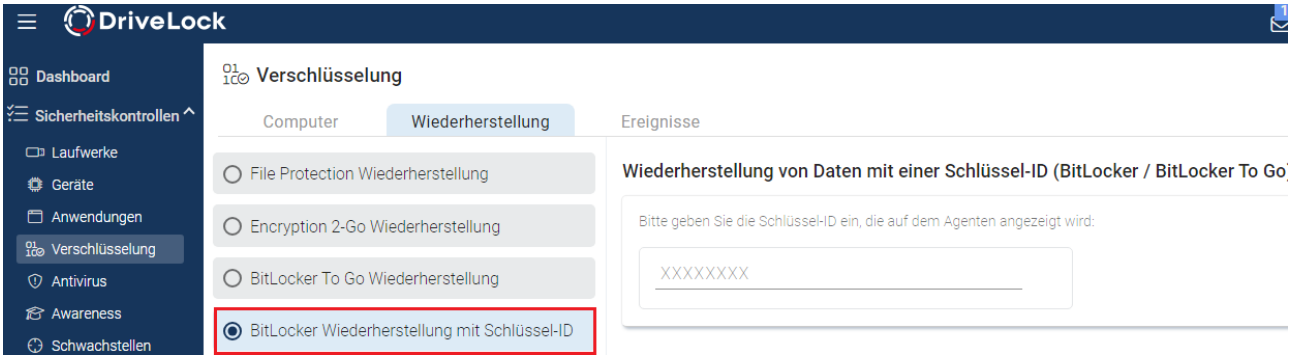
Weitere Informationen zu Zertifikaten finden Sie hier. Sobald der Wiederherstellungsschlüssel angezeigt wird, gehen Sie wie hier ab Schritt 8 beschrieben vor.

2.6.3.1 Wiederherstellung mit Schlüssel-ID

Eine Wiederherstellung mittels Challenge/Response ist auch dann möglich, wenn kein DriveLock Agent auf einem Client-Rechner installiert oder die ursprüngliche Zuordnung zu einem Endpoint unbekannt ist.

Helpdesk-Mitarbeiter können hier durch Eingabe der beim Endbenutzer angezeigten Schlüssel-ID dennoch einen Wiederherstellungsvorgang durchführen.

Dazu wird in den Sicherheitskontrollen im Menü **Verschlüsselung** auf dem Tab **Wiederherstellung** folgende Option gewählt:



2.7 Übernahme

2.7.1 Übernahme bestehender BitLocker-Umgebungen

Festplatten und Datenlaufwerke von Client-Computern, die bereits im Vorfeld mit original BitLocker verschlüsselt wurden, können jetzt ohne großen Aufwand in DriveLock BitLocker Management übernommen werden. Dadurch können Sie von zentraler Stelle aus die Ver- und Entschlüsselung mit BitLocker steuern und müssen sich nicht um den Verschlüsselungszustand einzelner Client-Computer kümmern.

Durch Setzen der Option **Vorhandene BitLocker-Umgebung verwalten** in Ihrer BitLocker-Richtlinie wird die Übernahme durch DriveLock festgelegt. Durch Zuweisen der Richtlinie auf die entsprechenden Client-Computer wird das BitLocker-Management aktiviert.

> Hinweis: Wenn Sie diese Option nicht setzen und in Ihrer Umgebung bereits mit original BitLocker verschlüsselte Laufwerke haben, ignoriert DriveLock diese. Sie bleiben weiterhin verschlüsselt, können aber nicht mit DriveLock BitLocker Management verwaltet werden.

Dabei unterscheiden sich Systemlaufwerke von Datenlaufwerken:

- **Systemlaufwerke:** Ein mit original BitLocker verschlüsseltes Systemlaufwerk wird von DriveLock automatisch übernommen und muss dabei nicht zwingend neu verschlüsselt werden. DriveLock passt im Hintergrund die Algorithmen an und tauscht Protektoren aus (auch External Keys werden gelöscht und neu erstellt). Stimmen die Verschlüsselungsalgorithmen überein, dann geht dies sehr schnell, während bei Nichtübereinstimmung eine Neuverschlüsselung erfolgt. Dies kann je nach System und Partitionsgröße eine längere Zeit in Anspruch nehmen.

  > Hinweis: Wenn die Option **Erst verschlüsseln, wenn Pre-Boot-Anmeldung einmal erfolgreich war** auf dem Reiter Verschlüsselungsschutz aktiviert wurde, muss das Laufwerk zunächst entschlüsselt werden. Nach erfolgreicher Anmeldung an der DriveLock-PBA wird das Laufwerk dann erneut verschlüsselt.

  Da der Benutzer durch seine Anmeldung am System bzw. Eingabe seines BitLocker-Kennworts das Systemlaufwerk direkt entsperrt, ist keine weitere Aktion seitens des Benutzers erforderlich.

- **Datenlaufwerke:** Datenpartitionen werden nicht automatisch entsperrt und von DriveLock übernommen. Die Benutzer müssen hier aktiv werden: Ein Assistent öffnet sich auf dem Client-Computer, in dem zunächst die Partition ausgewählt wird, die entsperrt werden soll. Anschließend muss das ursprüngliche BitLocker-Kennwort zum Entsperren des Datenlaufwerks eingegeben und dann ein neues Kennwort vergeben werden. Voraussetzung hierfür ist, dass Sie die Option **Benutzer muss Kennwort ändern** im Dialog **Kennwortoptionen** auswählen. Wenn Sie in diesem Dialog ein Kennwort vorgeben, müssen Sie dem Benutzer Ihre Kennwortvorgaben mitteilen. Benutzer müssen in diesem Fall kein neues BitLocker-Kennwort in dem Assistenten vergeben, sondern nur die zu entsperrenden Partitionen auswählen und das ursprüngliche Kennwort zum Entsperren eingeben.

Wiederherstellungsschlüssel: DriveLock BitLocker Management erstellt auch neue Wiederherstellungsschlüssel bei der Übernahme von original BitLocker-Umgebungen.

Verschlüsselungsalgorithmen: Wenn Sie sich an die Windows-Standardeinstellungen für Verschlüsselungsalgorithmen halten, kann die Übernahme bestehender BitLocker-Umgebungen problemlos und zügig durchgeführt werden.

2.7.2 Nachträgliche Anpassung von BitLocker-Richtlinien

In folgenden Fällen müssen Sie eine bestehende BitLocker-Richtlinie nachträglich anpassen:

- wenn sich an den Client-Computern, auf die die bestehende BitLocker-Richtlinie zugewiesen ist, etwas geändert hat (z.B. Laufwerksänderungen) oder
- wenn sich die Einstellungen für die Ver- oder Entschlüsselung geändert haben oder
- wenn Sie Ihre DriveLock Agenten auf einen höhere Version aktualisieren. Weitere Informationen zum Update des DriveLock Agenten finden Sie in den Release Notes.

Je nach Einstellung in der betreffenden Richtlinie ändert sich das Verschlüsselungsverhalten.

Hinweis: Die Änderungen an einer Richtlinie werden bei der nächsten Konfigurationsaktualisierung übernommen.

Folgende Möglichkeiten gibt es dabei:

- **Neuverschlüsseln bereits verschlüsselter Partitionen**
  Bei einer Änderung des Verschlüsselungsalgorithmus in der Richtlinie entschlüsselt das System die Partition zuerst und verschlüsselt sie dann sofort wieder unter Verwendung des neu eingestellten Algorithmus.
  Wenn Sie beispielsweise für Laufwerk E: den Algorithmus AES 128 Bit Schlüssellänge eingestellt hatten und diesen jetzt in AES-XTS 128 Bit Schlüssellänge ändern, wird neu verschlüsselt.
- **Austausch der Protektoren bereits verschlüsselter Partitionen ohne Neuverschlüsselung**
  Diese Vorgehensweise wird angewendet, wenn der Verschlüsselungsalgorithmus bereits mit dem in der Richtlinie eingetragenen Algorithmus übereinstimmt.
  Für die Änderung kann es zwei Ursachen geben:
  - Im ersten Fall führt der Wechsel von TPM/PIN zu TPM oder umgekehrt zum Austausch der Protektoren
  - Im zweiten Fall müssen bestehende BitLocker-Partitionen übernommen werden, die bereits mit dem in der Richtlinie eingetragenen Algorithmus verschlüsselt sind
- **Entschlüsseln von Partitionen**
  Ein Entschlüsseln wird immer dann angestoßen, wenn entweder
  - die Option **Lokale Festplatten auf Agenten-Computern verschlüsseln** deaktiviert wird oder
  - bei der Option **Einstellungen pro Laufwerk konfigurieren** ein Laufwerk nachträglich auf **Nicht verschlüsselt** gesetzt wird.

- wenn in den Lizenzoptionen unter **Lizenzierte Computer** die Option **Bitlocker Management** deaktiviert wird.

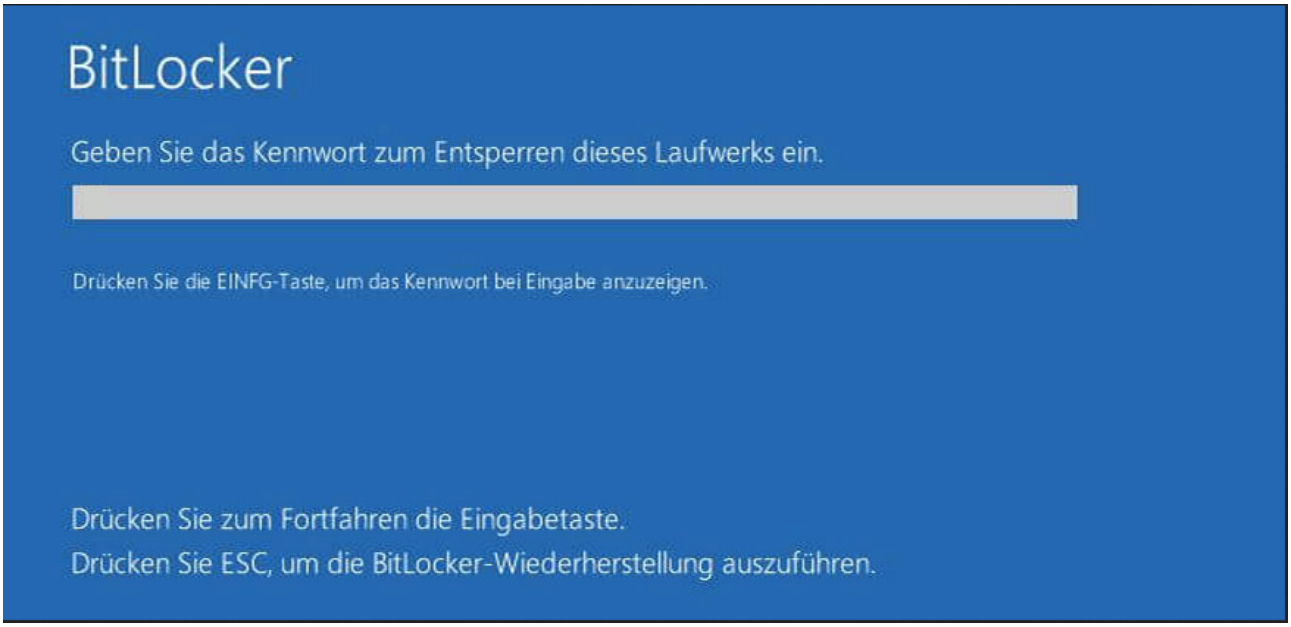
- **Verschlüsseln neu hinzugekommener Partitionen**
  Eine Verschlüsselung sollte immer dann angestoßen werden, wenn neue Hardware hinzukommt oder ein Laufwerk hinzugefügt wird (in der Option **Einstellungen pro Laufwerk konfigurieren**). Damit stellen Sie sicher, dass die Daten auf alle neuen Computer und Laufwerken durch BitLocker geschützt sind.

2.8 DriveLock Agent

2.8.1 Anmeldung an BitLocker

Bitte beachten Sie, dass bei der Anmeldung an der BitLocker-PreBootAuthentication (siehe Abbildung unten) ein **englisches Tastaturlayout** aktiv sein kann. Im Zweifel können Sie sich das eingegebene Kennwort anzeigen lassen, in dem Sie die EINFG-Taste drücken.

Achtung: Bitte teilen Sie den Benutzern diese Information mit und weisen sie darauf hin, dass Sonderzeichen auf einer EN-US Tastatur durch andere Tastenkombinationen belegt sind, sowie Y und Z vertauscht sind.

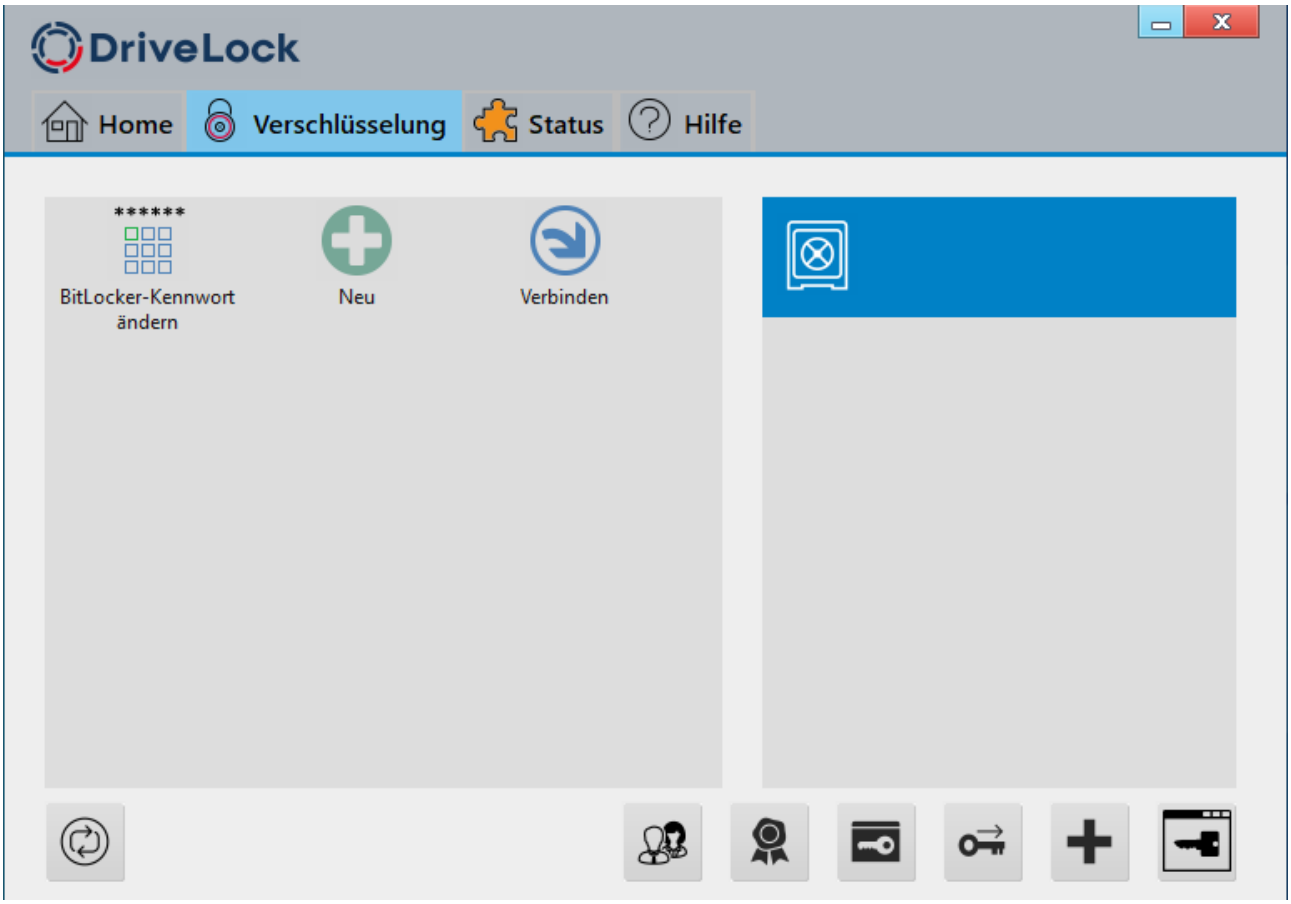


2.8.2 BitLocker Management auf Client-Computern (DriveLock Agent)

Mit der Zuweisung Ihrer BitLocker-Richtline auf die entsprechenden Client-Computer wird die Festplattenverschlüsselung initiiert. Je nach Ihren Kennwortvorgaben in den Einstellungen für die Pre-Boot-Authentifizierung erfolgt dies entweder mit oder ohne Kennworteingabe des jeweiligen Benutzers.

Hinweis: Bitte teilen Sie den Benutzern die entsprechenden Informationen für die Kennwortvergabe mit.

Auch besteht die Möglichkeit, dass der Benutzer das Kennwort nachträglich ändern darf. Auf dem Client-Computer wird dazu im **DriveLock Agent** auf dem Reiter **Verschlüsselung** die Schaltfläche **BitLocker-Kennwort ändern** angezeigt.



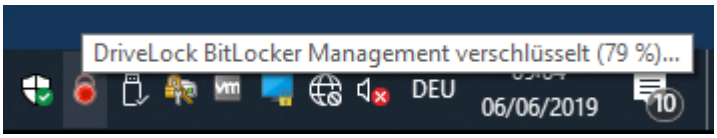
2.8.3 Verschlüsselung auf Client-Computern durchführen

Die Festplattenverschlüsselung auf den Client-Computern und die dazugehörige Kennworteingabe wird folgendermaßen durchgeführt:

1. In einem Fall startet der Benutzer seinen (noch unverschlüsselten) Client-Computer und meldet sich wie üblich an Windows an. Im anderen Fall ist der Benutzer bereits angemeldet, und der DriveLock Agent bekommt die neue BitLocker Richtlinie zugewiesen.
2. Dann gibt es zwei Möglichkeiten:

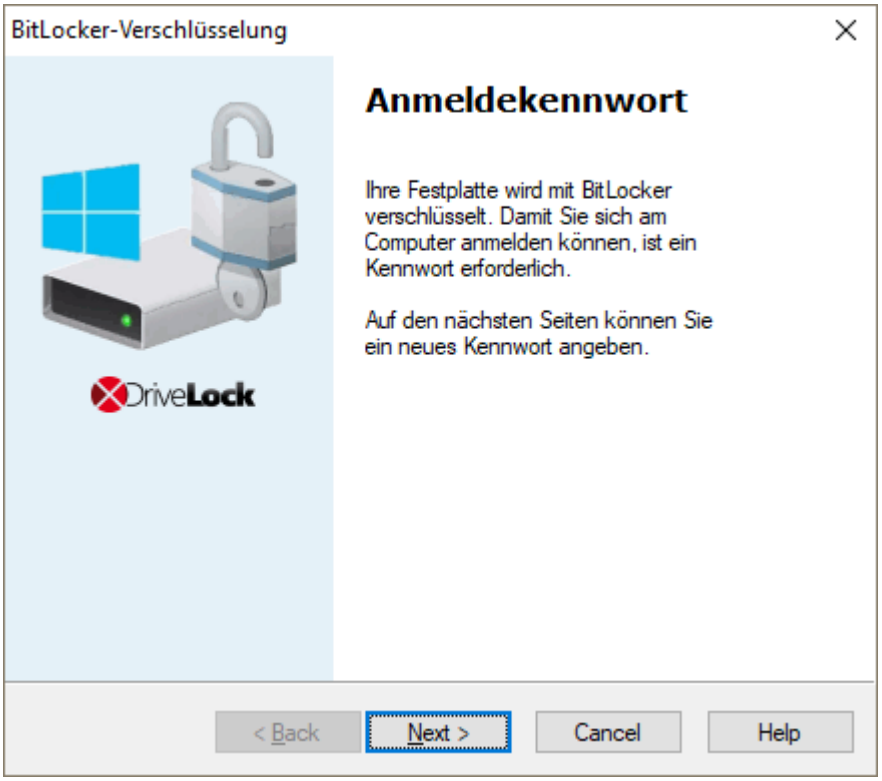
a. Wenn Sie ein festes Kennwort vorgegeben haben, startet die Verschlüsselung sofort, ohne dass dem Benutzer weitere Dialoge angezeigt werden.

   Lediglich in der Statusleiste kann der Verschlüsselungsprozess verfolgt werden:



   Nach Beenden der Verschlüsselung erscheint die in Punkt 5. beschriebene Meldung.

b. Wenn der Benutzer ein eigenes Kennwort vergeben muss, wird der Assistent zur Vergabe des BitLocker-Kennworts gestartet.



3. Im Fall b. vergibt der Benutzer nun ein Kennwort. Dabei werden die Richtlinienvorgaben geprüft und nur gültige Kennwörter akzeptiert.
4. Sobald die Kennwortvergabe abgeschlossen ist, beginnt der Verschlüsselungsprozess.
5. Wenn der Verschlüsselungsprozess beendet ist, erscheint folgende Meldung:

6. Beim nächsten Start des Client-Computers muss das BitLocker-Kennwort als Pre-Boot-Authentifizierung eingegeben werden, so dass die verschlüsselte Systempartition (und ggf. auch die Datenpartitionen) entsperrt wird.

   Im Fall a. wird der Client-Computer ohne Kennworteingabe gestartet.

2.8.3.1 Verschlüsselung verzögern

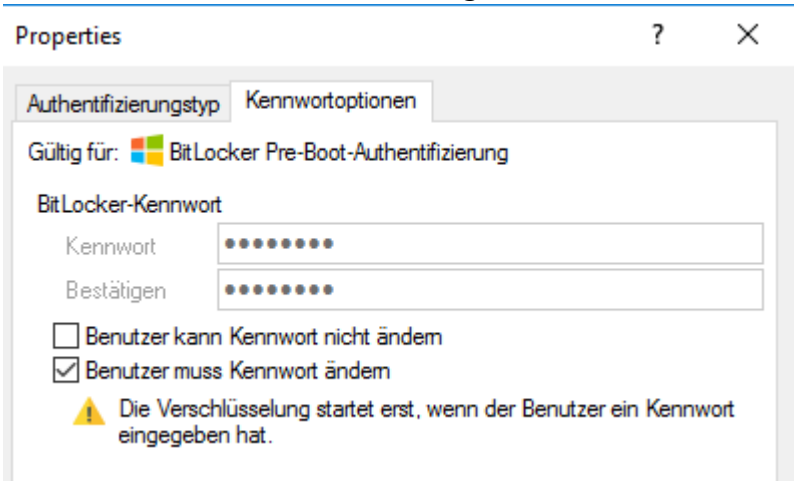
Benutzer können die Verschlüsselung hinausschieben, in dem sie in der Benachrichtigung (s. Abbildung) eine Zeit auswählen. Je nachdem, wie viele Stunden als Maximalwert in den Ausführungsoptionen angegeben sind, kann der Benutzer unter **Verzögern um** die Zeit bis zur nächsten Anzeige des Dialogs festlegen. So lange wird die Verschlüsselung dann aufgeschoben. Wenn der angegebene Maximalwert aufgebraucht ist, startet die Verschlüsselung. Sie startet auch, wenn der Benutzer während der Anzeige des Dialogs nichts tut oder auf **Verschlüsseln** klickt.


DriveLock
DriveLock
BitLocker Management
Ihr Computer wird verschlüsselt.
Die Verschlüsselung kann Ihre Rechnerleistung beeinträchtigen. Bei Bedarf können Sie deshalb den Zeitpunkt der Verschlüsselung hinauszögern. Wählen Sie hierzu eine Verzögerungszeit aus der Dropdown-Liste aus (je nach Vorgabe Ihres Administrators) und klicken Sie die Schaltfläche Später.
Um die Verschlüsselung sofort zu starten, klicken Sie die Schaltfläche Verschlüsseln.
Verschlüsselung starten in
4:52
Verzögern um
10Min.
Später
Verschlüsseln

2.8.4 Datenpartition mit vorhandenem BitLocker übernehmen

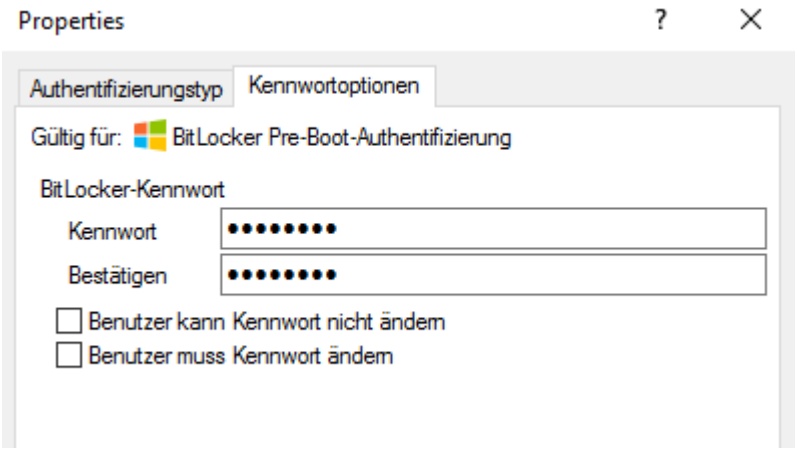
Das Vorgehen zum Entsperren von Datenpartitionen, die mit original BitLocker verschlüsselt wurden, und in DriveLock BitLocker Management übernommen werden sollen, richtet sich nach zwei Einstellungen in den **Kennwortoptionen** der BitLocker-Richtlinie:

- Ein BitLocker-Kennwort muss vergeben werden



oder

- das BitLocker-Kennwort ist vorgegeben.



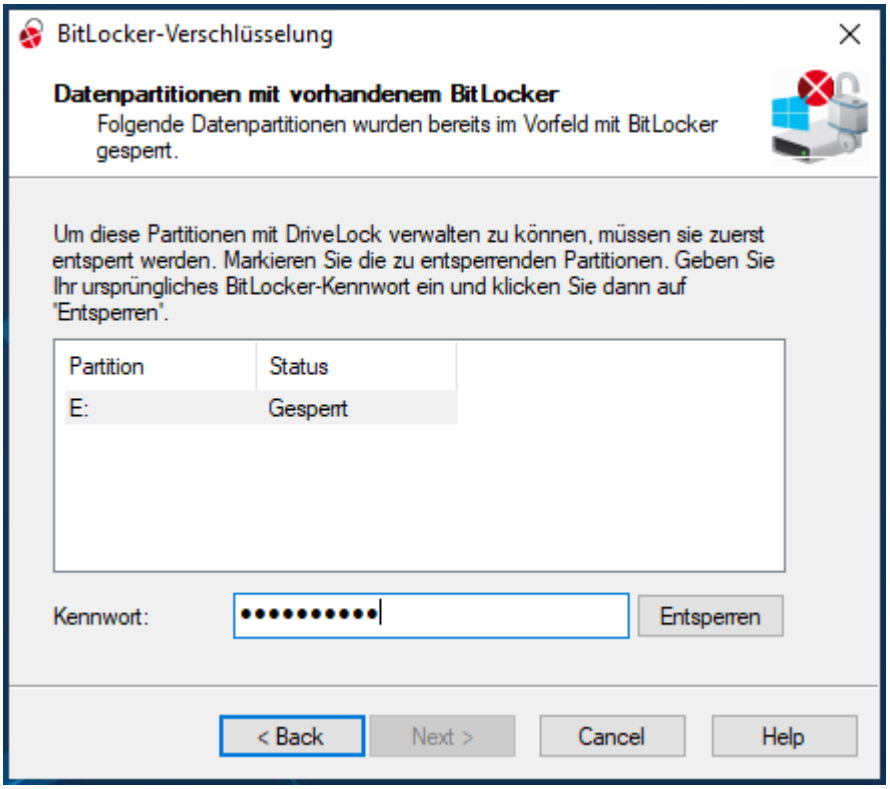
Je nachdem, welche Option ausgewählt wurde, öffnet sich am Client-Computer ein anderer Assistent.

- Bei einem Assistenten wird der Benutzer angewiesen, das Kennwort auf den folgenden Dialogseiten zu ändern.

- Der andere Assistent enthält lediglich Information zur Übernahme der bestehenden BitLocker-Umgebung:

In beiden Fällen muss auf der zweiten Dialogseite die Datenpartition ausgewählt werden, die entsperrt werden soll.

Hier muss das zu entsperrende Laufwerk (oder die Laufwerke) ausgewählt und in jedem Fall das original **Kennwort** eingegeben werden. Erst dann kann **Weiter** geklickt werden:



Wenn eine Kennwortneuvergabe erforderlich ist, erscheint anschließend ein weiterer Dialog, in dem ein neues Kennwort vergeben werden muss.

Den jeweiligen Abschlussdialog schließen Sie mit **Fertigstellen** ab.

Hinweis: Im Hintergrund wird dann die Übernahme durch DriveLock BitLocker Management vollzogen, indem Protektoren ausgetauscht und Verschlüsselungsalgorithmen übernommen werden.

2.9 BitLocker-Aktionen nachverfolgen

Im DriveLock Operations Center (DOC) können anhand von Ereignissen sämtliche BitLocker-Aktionen nachverfolgt werden.

Eine weitere Möglichkeit bietet Ihnen eine detaillierte Diagnoseprotokollierung mittels Tracing. Dies kann beispielsweise wichtig sein, um Fehler bei der Übernahme von original BitLocker-Umgebungen nachzuvollziehen. Die entsprechende Datei hat den Namen `DlSvcBitLocker.log`, siehe Abbildung unten. Hier lässt sich genau ersehen, welche Aktionen DriveLock bei der Übernahme von bestehenden BitLocker-Umgebungen durchführt.

Sie können die Erzeugung von Trace-Dateien über die Kommandozeile, mit Hilfe der DriveLock Management Konsole oder über das DriveLock Support-Tool `DLSupport.exe` (befindet sich im Installationsverzeichnis von DriveLock) aktivieren.

3 DriveLock Pre-Boot-Authentifizierung

Die DriveLock Pre-Boot-Authentifizierung (PBA) kann für beide DriveLock Verschlüsselungstechnologien - BitLocker und Disk Protection (Full Disk Encryption, FDE) - verwendet werden. Der Einsatz der DriveLock Pre-Boot-Authentifizierung für BitLocker erfordert eine Lizenz.

Achtung: Bitte beachten Sie, dass die PBA ausschließlich auf UEFI Systemen ab Windows 10 Umgebungen funktioniert.

Hinweis: Da ab Version 2022.2 die DriveLock Legacy BIOS Pre-Boot Authentifizierung nicht mehr unterstützt wird, wird bei der Installation eines Agenten geprüft, ob eine aktive Legacy BIOS PBA auf dem System vorhanden ist. In diesem Fall wird keine Aktualisierung bzw. Installation des Agenten durchgeführt.

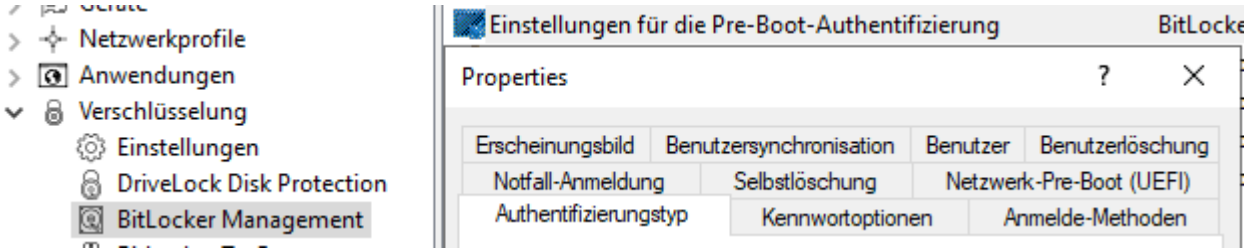
Die DriveLock Pre-Boot-Authentifizierung bietet Ihnen eine Reihe von Vorteilen:

- Anmeldung mit Benutzernamen / Kennwort
- Wiederherstellung über Challenge-Response Verfahren
- Single Sign-on (SSO) zur Windows Anmeldung
- Anmeldung mit Smartcard
- Unterstützung anderer Tastatur-Layouts und virtuelles Keyboard
- Wechselbare PBA-Hintergrundbilder

3.1 Einstellungen für die Pre-Boot-Authentifizierung

Diese Einstellungen können sowohl für Disk Protection als auch für BitLocker Management gesetzt werden. Bitte beachten Sie dabei, dass die DriveLock PBA für BitLocker Management eine separate Lizenz auf Basis der BitLocker Management Lizenz erfordert.

Für BitLocker Management sind folgende Einstellungen konfigurierbar:



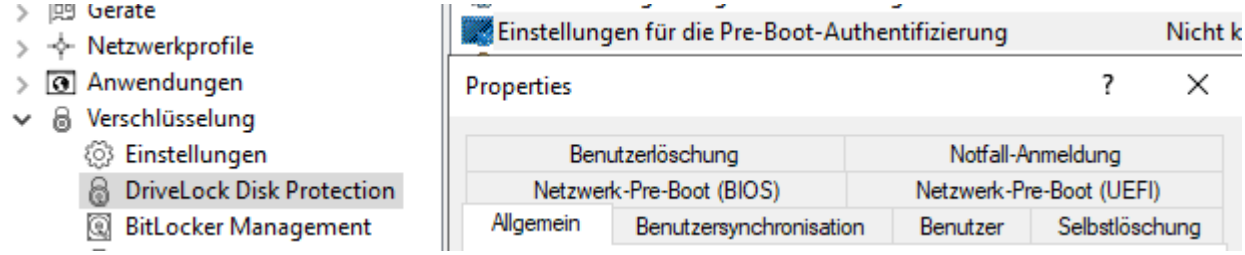
Anmelde-Methoden

Authentifizierungstyp

Erscheinungsbild

Kennwortoptionen

Für Disk Protection sind folgende Einstellungen konfigurierbar:



Allgemein

Netzwerk-Pre-Boot (BIOS)

Auf folgenden Reitern sind die Einstellungen für beide Module konfigurierbar:

Benutzer

Benutzersynchronisation

Benutzerlöschung

Netzwerk-Pre-Boot (UEFI)

Notfall-Anmeldung

Selbstlöschung

3.1.1 Benutzer

Auf diesem Reiter nehmen Sie Einstellungen zu den Benutzern der DriveLock PBA vor.

- DriveLock fügt jeden Benutzer zur Pre-Boot-Authentifzierungs-Datenbank hinzu, der erfolgreich an Windows angemeldet wurde. Aus diesem Grund ist die Option **Windows-Benutzer automatisch zur Pre-Boot-Authentifizierung hinzufügen** standardmäßig gesetzt. Durch Abwahl dieser Option werden die Benutzer nicht mehr automatisch hinzugefügt.
  Über die Schaltflächen **Hinzufügen**, **Entfernen** oder **Bearbeiten** können Sie bestehende Benutzer ändern, entfernen oder neue Benutzer zur Datenbank hinzuzufügen.

  Hinweis: Für einen PBA-Benutzer muss nicht unbedingt ein Windows Benutzerkonto existieren, Sie können zusätzliche Anmeldedaten (Benutzername / Kennwort) nur für die Pre-Boot-Authentifizierung erstellen (z.B. ein Notfallkonto).

- Wenn Sie die Option **Immer Downlevel-Logon-Namen während Single-Sign-on verwenden** aktivieren, ist die Benutzeranmeldung nur noch mit den sogenannten Downlevel-Logon-Namen möglich. Diese haben die Form "DOMAIN\Benutzername". Eine Anmeldung mit benutzername@domain.org (sog. User-Principal Names) ist damit nicht mehr zugelassen.

3.1.2 Benutzersynchronisation

Die Option **Active Directory-Benutzer zur Pre-Boot-Authentifizierung synchronisieren** ist standardmäßig nicht aktiviert, da AD-Benutzer automatisch in die PBA Datenbank eingetragen werden, sobald sie sich an der PBA anmelden.

Hinweis: Verwenden Sie diese Option nur, wenn Sie die PBA vorkonfigurieren wollen, indem Sie Benutzer manuell aus dem AD bereits vor deren Anmeldung in die PBA-Benutzerdatenbank aufnehmen.

Fügen Sie in diesem Fall die entsprechenden AD-Gruppen und -Benutzer hinzu, die Sie in die PBA-Datenbank synchronisieren wollen.

Hinweis: Bitte beachten Sie, dass die Mitglieder der Gruppe "Domänen-Benutzer" nicht synchronisiert werden. Diese Gruppe verwendet einen "berechneten" Mechanismus, der auf der "primären Gruppen-ID" des Benutzers basiert, um die Mitgliedschaft zu bestimmen, und speichert Mitglieder normalerweise nicht als mehrwertige verknüpfte Attribute.

Als initiales Kennwort können Sie ein **festes Kennwort** (identisch für alle Benutzer), den **Benutzernamen** oder jeden verfügbaren **Wert von AD-Eigenschaft** vergeben.

Hinweise zu Disk Protection:

DriveLock unterscheidet bei Disk Protection vier Typen von Pre-Boot-Nutzern:

Hinzugefügt über	Beschreibung
DlFdeUser	Benutzer wurde lokal mit `DlFdeUser.exe` erstellt
Richtlinie	Benutzer wurde über die Richtlinie erstellt - und wird mit Änderungen der Richtlinie synchronisiert/entfernt.
Windows-Anmeldung	Benutzer wurde durch Windows-Login erstellt - das Kennwort wird bei jedem erfolgreichen Windows-Login synchronisiert.
Active Directory	Benutzer wurde aus AD-Gruppen synchronisiert - und wird gelöscht, wenn er aus der AD-Gruppe bzw. Benutzersynchronisation gelöscht wird. Das Kennwort wird bei jedem erfolgreichen Windows-Login lokal synchronisiert.

- Das Kommando `DlFdeUser.exe` kann auch andere Benutzertypen löschen. Diese werden beim nächsten Windows-Login oder Laden der Richtlinie wieder hinzugefügt.
- Windows-Benutzer, die sich zum ersten Mal an einem Client-Computer anmelden, der mit DriveLock Disk Protection und Pre-Boot-Authentifizierung (PBA) geschützt ist, sind mit ihren Windows-Anmeldedaten noch nicht in der PBA-Datenbank synchronisiert. Sie müssen sich an der PBA entweder mit einem vorkonfigurierten Benutzer anmelden, der über DlFde oder die Richtlinie hinzugefügt wurde, oder ein anderer berechtigter Benutzer meldet sich an der PBA an, um den Windows-Anmeldedialog anzuzeigen.
- Benutzer, die über das AD hinzugefügt wurden, werden jedes Mal synchronisiert, wenn die Richtlinie geladen wird. Fügen Sie Benutzer zu den konfigurierten AD-Gruppen hinzu oder entfernen Sie diese, werden bei der nächsten Synchronisation auf allen betroffenen PCs diese Benutzer auch in der PBA-Datenbank hinzugefügt/entfernt.

3.1.3 Benutzerlöschung

Zum Konfigurieren der Benutzerlöschung wählen Sie den Reiter **Benutzerlöschung**, markieren **Benutzer-initiiere Löschung aktivieren** und geben ein Lösch-Suffix ein.

Durch Aktivierung dieser Option ist es einem gültigen PBA-Benutzer erlaubt, das System unzugänglich zu machen.

3.1.4 Netzwerk-Pre-Boot (UEFI)

Informationen zu diesem Reiter finden Sie hier.

3.1.5 Notfall-Anmeldung

Diese Einstellungen geben an, welche Anmeldeverfahren zur Verfügung stehen, wenn ein Benutzer nicht mehr in der Lage ist, sich an der DriveLock PBA anzumelden (z.B. Kennwort vergessen).

Wir empfehlen, die Standardeinstellungen zu verwenden.

- **Notfall-Anmeldung mit Benutzername**: Diese Standardoption ermöglicht eine Notfall-Anmeldung des Benutzers unter Angabe seines Namens. Das betrifft Windows-Domänen oder lokale Windows-Benutzer Kennwort-Accounts, die der PBA-Benutzerdatenbank hinzugefügt wurden. Es erlaubt einen einmaligen Pre-Boot Zugriff auf das System.

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

- **Single-Sign-on nach Notfall-Anmeldung** ermöglicht es Benutzern, sich an Windows anzumelden und damit zu arbeiten, wenn sie ihr Kennwort vergessen haben - auch wenn ein Administrator das Kennwort noch nicht zurückgesetzt hat.
- **Notfall-Anmeldung ohne Benutzername** ermöglicht einen einmaligen Pre-Boot Zugriff auf das System für alle Benutzer, die noch niemals am System angemeldet waren. Single-Sign-on (SSO) ist in diesem Fall dann nicht möglich.
- Bitte beachten Sie bei Aktivierung der Option **Notfall-Anmeldung für Benutzer von Token-Geräten**, dass die entsprechenden Einstellungen für Anmeldung mit Tokens auf dem Reiter **Anmelde-Methoden** (für BitLocker Management) bzw. **Allgemein** (für Disk Protection) vornehmen.

  Hinweis: Wenn diese Option aktiviert ist, sind Smartcard/Token-Benutzer (die ihr Token verlegt oder ihre PIN vergessen haben) berechtigt, das Verfahren für die Notfall-Anmeldung für Token-Benutzer aufzurufen. Dieses Verfahren

erlaubt einen einmaligen Pre-Boot Zugriff auf das System ohne Nutzung eines Tokens.

3.1.6 Selbstlöschung

Die Selbstlöschung hat hauptsächlich zwei Anwendungsszenarien. Entweder möchten Sie die Daten auf einem verloren gegangenen PC schützen, der sich nicht mehr mit dem DES verbindet und/oder Sie wollen mobile Benutzer dazu zwingen sich regelmäßig mit dem Firmennetz zu verbinden.

Zum Konfigurieren der Selbstlöschung wählen Sie den Reiter **Selbstlöschung**, markieren **Selbstlöschung aktivieren, wenn der Computer offline ist** und konfigurieren die für Sie geeigneten Einstellengen wie im Dialog beschrieben.

Nach Ablauf der angegebenen Offline-Zeit löscht DriveLock die PBA-Datenbank.

3.2 Einstellungen in der Listenansicht für die PBA

Für die Pre-Boot-Authentifizierung gibt es drei Einstellungen, die in den Knoten **DriveLock Disk Protection** und **BitLocker Management** nur in der Listenansicht zu finden sind.

Diese sind:

- Änderungen der lokalen PBA-Konfiguration zulassen
- PBA-Tastaturtreiber auswählen
- SmartCard-Treiber in PBA laden

3.2.1 Änderungen der lokalen PBA-Konfiguration zulassen

Mit dem Kommandozeilenprogramm 'dlsetpb.exe' können Sie auf einem Computer Anpassungen an der PBA-Konfiguration vornehmen.

Diese Einstellung bestimmt, ob diese Konfigurationsänderungen bei der nächsten Aktualisierung der Richtlinie beibehalten oder überschrieben werden (mit den Einstellungen aus der Richtlinie, z.B. welcher Tastaturtreiber verwendet werden soll). Standardmäßig werden die Änderungen des Kommandozeilenprogramms beibehalten.

Hinweis: Beim Update von einer Version vor 2020.2 werden alle Einstellungen so behandelt, als wären sie vom Kommandozeilenprogramm gesetzt worden.

3.2.2 PBA-Tastaturtreiber auswählen

Mit dieser Einstellung können Sie den Tastaturtreiber für die PBA festlegen.

Wenn der verwendete Standardtreiber beispielsweise keine unterschiedlichen Tastaturlayouts kennt, können Sie hier einen Treiber von DriveLock auswählen. Der Kombi-Treiber kombiniert sowohl Tastatur- als auch Maustreiber in einem. Wenn dieser nicht zum gewünschten Resultat führt, können Sie auch den (älteren) DriveLock-Tastaturtreiber verwenden.

Hinweis: Beachten Sie, dass Sie möglicherweise auf unterschiedlichen Geräte unterschiedliche Treiber einstellen müssen.

3.2.3 SmartCard-Treiber in PBA laden

Hiermit geben Sie an, ob der DriveLock-SmartCard-Treiber verwendet werden soll.
Wenn Sie SmartCards einsetzen wollen und der Standardtreiber diese nicht erkennt, können Sie diese Einstellung verwenden.

Hinweis: Beachten Sie, dass Sie möglicherweise auf unterschiedlichen Geräte unterschiedliche SmartCard-Treiber einstellen müssen.

Achtung: Für die DriveLock PBA werden SmartCard-Leser vorausgesetzt, die eine CCID V1.1 konforme Schnittstelle haben.

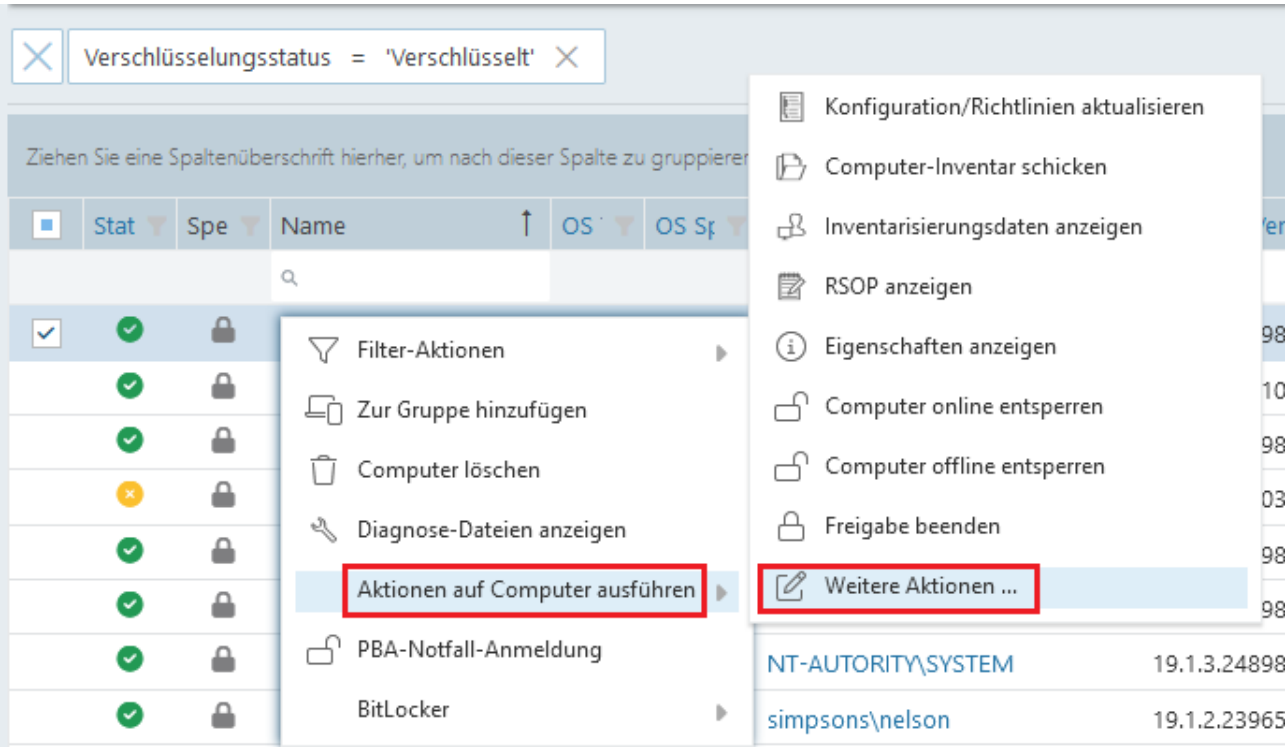
3.3 PBA-Einstellungen im DriveLock Operations Center (DOC)

Es kann sinnvoll sein, die PBA zu deaktivieren, beispielsweise wenn Aktualisierungen anstehen, die einen Neustart erfordern.

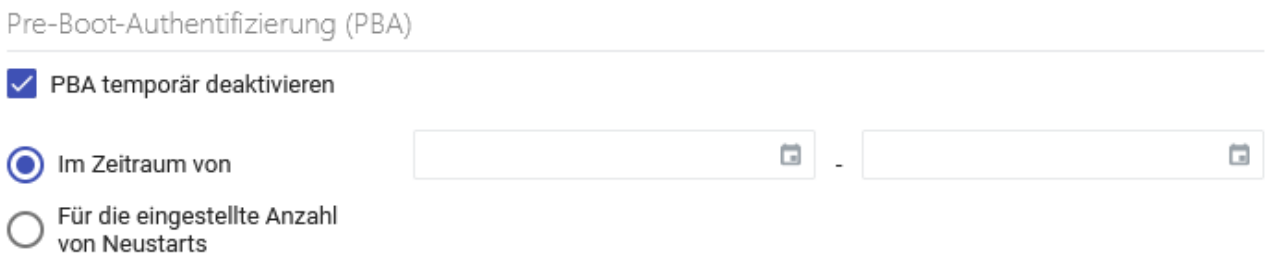
Hinweis: Diese Einstellung gilt sowohl für die DriveLock- als auch für die BitLocker-PBA.

Öffnen Sie im DOC das Dashboard **Verschlüsselung**. Rufen Sie eine Liste der verschlüsselten Computer entweder über das Widget **Verschlüsselungsstatus** oder das Widget **Verschlüsselungsinformation** auf. Wählen Sie den entsprechende Computer. Sie können diesen auch direkt in der **Computer** Ansicht auswählen.

Wählen Sie im Kontextmenü **Aktionen auf Computer ausführen** und dann **Weitere Aktionen**. Im darauffolgenden Dialog wählen Sie **Alle Aktionen anzeigen**.



Setzen Sie im Bereich Pre-Boot-Authentifizierung bei PBA temporär deaktivieren ein Häkchen und scrollen dann etwas herunter, um sich die Einstellungen anzeigen zu lassen:



Sie können diese Einstellung für eine bestimmte Anzahl an Neustarts oder für einen bestimmten Zeitraum angeben. Diese Aktion wird einmalig definiert, d.h. sie kann jederzeit erneuert werden.

Der Status wird bei den Computer-Details angezeigt.

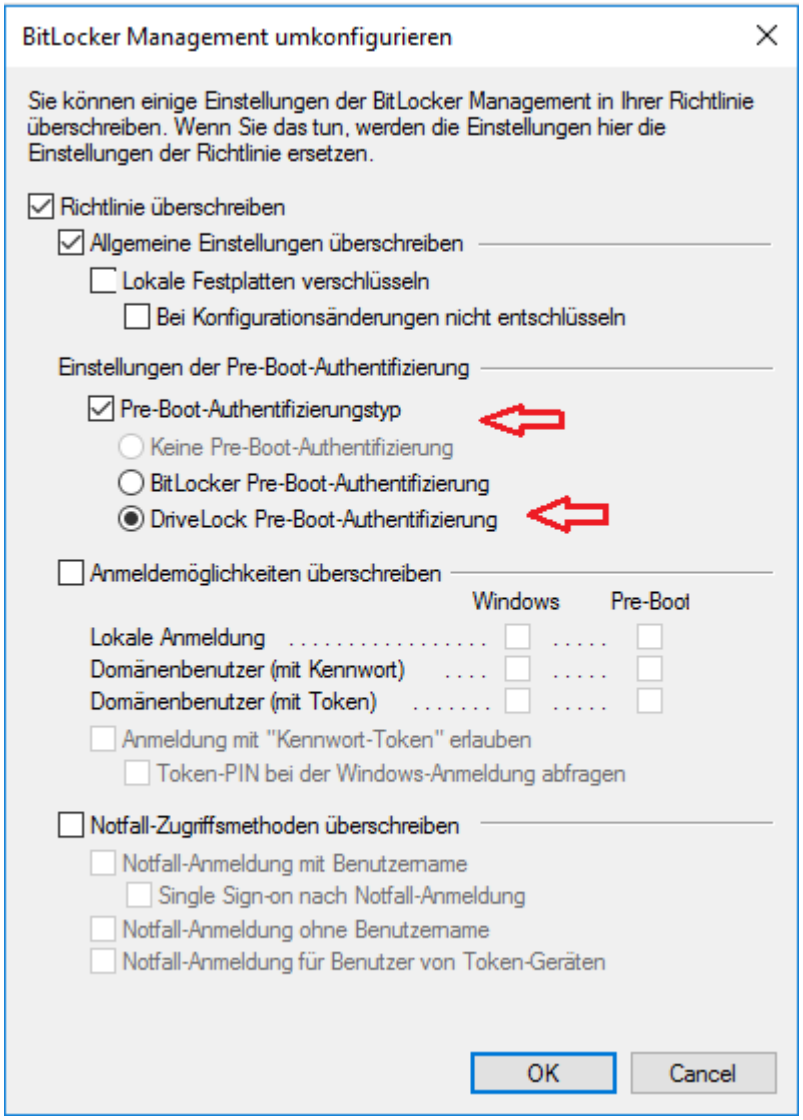
3.4 Richtlinie überschreiben (DriveLock PBA)

Um auf einzelnen Client-Computern gezielt Pre-Boot-Authentifizierungsseinstellungen außer Kraft zu setzen, können Sie bereits gesetzte Richtlinieneinstellungen überschreiben.

Achtung: Beachten Sie bitte, dass die Richtlinieneinstellungen erst dann wieder aktiv werden, wenn Sie die Überschreibungsoption wieder rückgängig gemacht haben.

Gehen Sie folgendermaßen vor:

1. Öffnen Sie die **Agenten-Fernkontrolle** im Knoten **Betrieb**.
2. Markieren Sie den Client-Computer, dessen Richtlinie Sie überschreiben wollen.
3. Wählen Sie aus dem Kontextmenü den Menüpunkt **Verschlüsselungs-Eigenschaften...**
4. Auf dem Reiter **Allgemein** sehen Sie Informationen zur Verschlüsselung des DriveLock Agenten. Klicken Sie auf die Schaltfläche **Agent umkonfigurieren...**.
5. Setzen Sie die Option **Richtlinie überschreiben** und lassen Sie die Option **Allgemeine Einstellungen überschreiben** angehakt (Standardeinstellung).



6. Wählen Sie im Abschnitt Einstellungen der Pre-Boot-Authentifizierung die jeweilige PBA aus.

> Hinweis: Wenn kein TPM vorhanden ist, ist die Option **Keine Pre-Boot-Authentifizierung** automatisch ausgegraut (siehe Abbildung oben).

7. Die Optionen **Anmeldemöglichkeiten überschreiben** und **Notfall-Zugriffsmethoden überschreiben** sind nur aktiv, wenn Sie DriveLock Pre-Boot-Authentifizierung ausgewählt haben. Bei beiden Optionen werden die entsprechenden Einstellungen in der Richtlinie überschrieben. Weitere Informationen finden Sie in den Kapiteln Anmelde-Methoden und Notfallanmeldung.
8. Wenn Sie jetzt **OK** klicken, werden Ihre Einstellungen mit sofortiger Wirkung auf dem gewählten Client-Computer angewendet.

3.5 Netzwerk-Pre-Boot-Authentifizierung (UEFI)

Dieser Zusatz zur DriveLock Pre-Boot-Authentifizierung ermöglicht eine vereinfachte Verwaltung von Client-Computern (Drivelock Agenten) in Netzwerk-Umgebungen.

Beim Neustart kann das jeweilige Betriebssystem-Laufwerk eines Client-Computers automatisch freigegeben werden, wenn dieser mit einem Unternehmensnetzwerk über Kabel verbunden ist. Dadurch lassen sich Client-Systeme, welche die Hardwareanforderungen erfüllen, ohne Benutzereingriff in Windows starten.

Das Feature lässt sich beispielsweise so konfigurieren, dass Client-Computer nur dann automatisch gestartet werden können, wenn sie sich im Netzwerk befinden. Kein Start ohne Netzwerk!

Sollte keine Netzwerkverbindung verfügbar sein, können Alternativen erlaubt werden (z.B. Notfall-Anmeldung mit Benutzer- und Kennworteingabe).

Für Administratoren erleichtert dies unter anderem auch das Ausrollen von Software-Patchen auf unbeaufsichtigte Client-Computer.

Beachten Sie folgende Einschränkungen:

- Es wird nur UEFI-Firmware unterstützt
- Es wird nur kabelgebundenes Netzwerk unterstützt
- Es werden nur Netzwerk-Adapter unterstützt, die UEFI für PXE Boot anbietet
- Die DriveLock Netzwerk-PBA liefert keine eigenen Netzwerktreiber mit

Folgende Regeln gelten:

- Die Netzwerk-PBA und der DriveLock Enterprise Service (DES) müssen das gleiche Datum / Uhrzeit haben

> Achtung: Bei einer Zeitumstellung (z.B. Winter- auf Sommerzeit) kann es zu einer Abweichung der Server- und Systemzeit kommen, wenn Ihre DriveLock Agenten vor der Umstellung heruntergefahren wurden (somit also die 'alte' Zeit verwenden), aber die Zeit auf Ihrem Server bereits umgestellt wurde. In diesem Fall wird die Anmeldung an der Netzwerk-PBA blockiert. Die Endbenutzer müssen einmalig eine andere Anmelde-Methode auswählen (Benutzername-/Kennworteingabe) bzw. die Systemzeit einstellen. Sobald beide Zeiten synchronisiert sind, wird die Anmeldung an der Netzwerk-PBA wieder funktionieren.

- Zum Aushandeln der Schlüsselpaare wird die sichere Netzwerkverbindung unter Windows zum DES vorausgesetzt (HTTPS/SSL)
- Verbindungen über Proxy werden in der Netzwerk-PBA nicht unterstützt
- Im DriveLock Operations Center (DOC) kann die automatische Anmeldung für jeden DriveLock Agenten temporär deaktiviert werden (weitere Informationen finden Sie hier)

> Achtung: Damit die Netzwerk-PBA funktioniert, muss in der Richtlinie eine Server-Verbindung im Knoten **Globale Einstellungen**, Unterknoten **Server-Verbindungen**, eingetragen sein.

3.5.1 Netzwerk-Pre-Boot (UEFI)

> Hinweis: Die Einstellungen auf dem Reiter **Netzwerk-Pre-Boot (UEFI)** sind je nach Lizenz sowohl für DriveLock Disk Protection, als auch für DriveLock BitLocker Management verfügbar, da in beiden Fällen die DriveLock Pre-Boot-Authentifizierung verwendet wird.

Folgende Einstellungen sind auf dem Reiter möglich:

1. Setzen Sie ein Häkchen bei der Option **Netzwerk-Pre-Boot-Authentifizierung aktivieren**, um das Feature zu aktivieren. Sie müssen jedoch zusätzlich mindestens eine der beiden unteren Optionen auswählen (automatische oder AD-Anmeldung).
2. Die Option **Automatische Anmeldung am Netzwerk erlauben** ermöglicht bei vorhandener Netzwerkverbindung eine Authentifizierung am Client Computer ohne Interaktion eines Benutzers.

Folgendes läuft im Hintergrund ab, sobald die Richtlinie mit dieser Einstellung dem DriveLock Agenten (Client Computer) zugewiesen ist:

- Anlage eines speziellen Netzwerk-Benutzers in der PBA-Datenbank ('AutoLogon-Benutzer') mit autogeneriertem Benutzerkennwort
- Austausch eines RSA-Schlüsselpaares zwischen DriveLock Agent und DriveLock Enterprise Service (DES)

Hinweis: Eine automatische Anmeldung an der PBA erfolgt nur wenn dieser Schlüsselaustausch erfolgreich stattfindet.

Achtung: Beachten Sie, dass das Client-Betriebssystem nur bei vorhandener Netzwerkverbindung zwischen DriveLock Agent und DES gestartet werden kann.

Siehe folgenden Anwendungsfall.

3. Bei Auswahl der automatischen Anmeldung ist standardmäßig immer die Option **Andere Anmeldemethoden zulassen** zusätzlich ausgewählt. Diese Option garantiert, dass eine Authentifizierung auch ohne Netzwerkverbindung möglich ist.

Achtung: Wenn Sie das Häkchen hier entfernen, existiert die Möglichkeit einer lokalen Anmeldung bzw. Anmeldung über Challenge-Response-Verfahren nicht mehr. Falls die Konfiguration ungültig wird, ist das System nicht mehr bootfähig. Alle Benutzerkonten werden dabei automatisch aus der PBA gelöscht, AD-Synchronisation und Benutzer-Import sind nicht mehr aktiviert!

4. Die Option **Anzahl der Netzwerk-Anmeldungen, die erfolgreich durchgeführt werden müssen, bevor die Ausfallsicherung deaktiviert wird** hat den Vorgabewert 3.
Hintergrund: Ein zusätzlicher lokaler AutoLogon-Benutzer wird in der Netzwerk-PBA konfiguriert, der als Ausfallsicherung dient, falls die Netzwerk-PBA nicht in der Lage sein sollte, über Netzwerk zu booten.
Nach den eingestellten erfolgreichen Netzwerk-Anmeldungen wird der lokale AutoLogon-Benutzer gelöscht und danach kann nur noch über den Netzwerk Autologon gebootet werden.

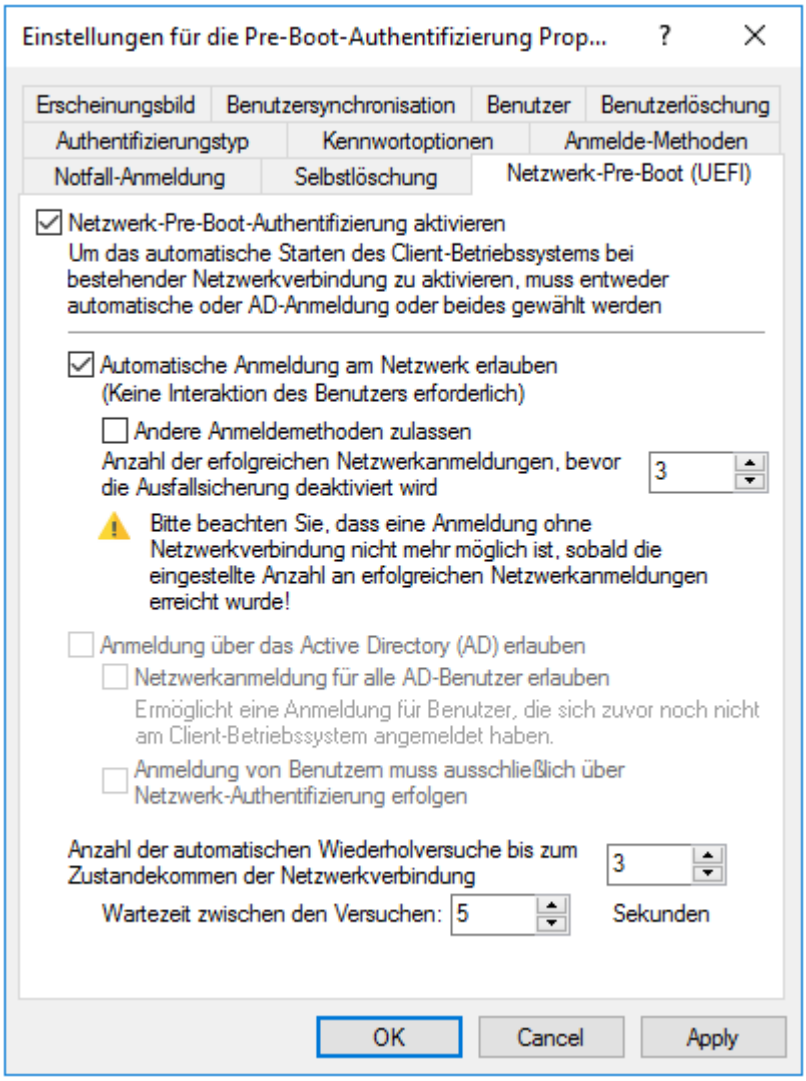
> Achtung: Diese Option kann nur initial gesetzt werden, sie hat keine Auswirkungen mehr auf bereits lauffähige Systeme. Aus Sicherheitsgründen sollten Sie darauf achten, die Zahl nicht zu hoch einzustellen.

5. **Anmeldung über das Active Directory (AD) erlauben**: Wählen Sie diese Option, um Anmeldeinformationen aus dem AD zu beziehen.
6. **Netzwerkanmeldung für alle AD-Benutzer erlauben**: Wählen Sie diese Option, um sicherzustellen, dass Benutzer angemeldet werden können, die zwar im AD bekannt sind, aber in der PBA-Datenbank noch nicht.
   Siehe folgenden Anwendungsfall.
7. **Anmeldung von Benutzer muss ausschließlich über Netzwerk-Authentifizierung erfolgen**: Die Netzwerk-PBA erlaubt nur Anmeldungen, wenn auch die Benutzeranmeldeinformationen gegenüber dem AD online geprüft werden können. Eine Netzwerkanmeldung ist somit Voraussetzung, ohne Netzwerk wird nur noch ein Challenge-Response-Verfahren angeboten.
8. **Anzahl der automatischen Wiederholversuche bis zum Zustandekommen der Netzwerkverbindung**: Geben Sie hier an, wie oft das System automatisch versuchen soll, eine Netzwerkverbindung herzustellen.
9. **Wartezeit zwischen den Versuchen**: Geben Sie hier die Sekunden an, die zwischen den Wiederholversuchen liegen darf. Standardwert ist 5 Sekunden.
   Beispiel: Um einem Router ausreichend Zeit zu geben, eine Netzwerkverbindung herzustellen, kann man die Anzahl der automatischen Wiederholversuche erhöhen und die Pause entsprechend anpassen. Eine Pause mit dem Wert 0 bedeutet, dass sofort wiederholt wird.

3.5.2 Anwendungsfall 1: Automatische Anmeldung

Es gibt spezielle Anwendungsfälle, bei denen das Betriebssystem eines Client Computers nur dann gestartet werden darf, wenn eine Netzwerkverbindung besteht, z.B. Geldautomaten oder spezielle Notebooks, die ausschließlich im Unternehmensnetzwerk verwendet werden dürfen. Im Fall, dass ein derartiger Rechner entwendet werden sollte, kann das Betriebssystem ohne Netzwerkverbindung nicht mehr gestartet und die Festplatten dementsprechend auch nicht mehr entschlüsselt werden.

Zur Konfiguration gehen Sie folgendermaßen vor (die Einstellungen auf den anderen Reitern entnehmen Sie bitte den jeweiligen Beschreibungen):



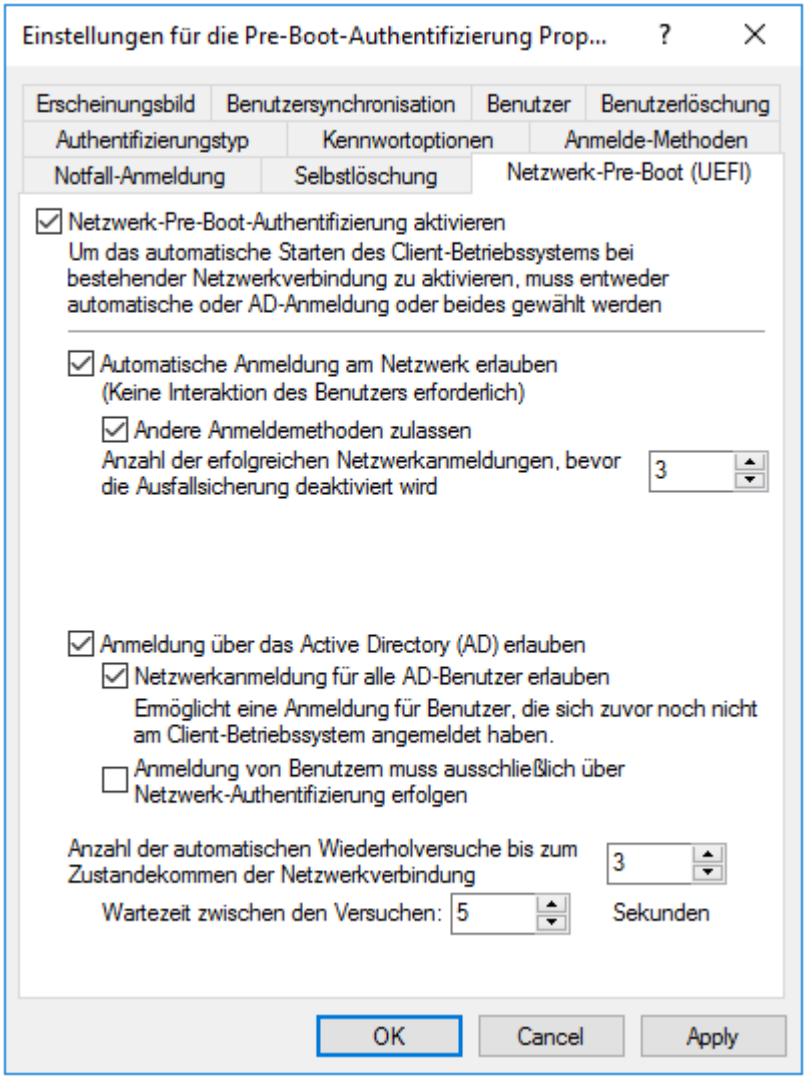
1. Wählen Sie die Grundeinstellung **Netzwerk-Pre-Boot-Authentifizierung aktivieren**.
2. Wählen Sie **Automatische Anmeldung am Netzwerk erlauben** aus.
3. Entfernen Sie das Häkchen bei **Andere Anmeldemethoden zulassen**.
4. Belassen Sie den Standardwert für die Ausfallsicherung bei 3. So können Sie sicherstellen, dass erst nach 3 erfolgreichen Netzwerk-Anmeldungen keine andere Möglichkeit mehr für eine Anmeldung besteht. Diese Option dient zum einen für Testzwecke und zum anderen als Ausfallsicherung.
5. Belassen Sie den Standardwert 3 bei **Anzahl der automatischen Wiederholversuche bis Zustandekommen der Netzwerkverbindung**.
6. Ebenso können Sie die Pausen zwischen den Wiederholversuchen bei 5 Sekunden lassen.
7. Klicken Sie die Schaltfläche **Bestätigen**, um Ihre Eingaben zu übernehmen und schließen Sie den Dialog mit **OK**.

3.5.3 Anwendungsfall 2: Netzwerkanmeldung für alle AD-Benutzer

Zwei Fälle:

- Ein Mitarbeiter (neuer Benutzer) muss sich an einem bestimmten Client-Computer in Windows anmelden, obwohl er sich dort noch nie angemeldet hat. Der Client-Computer ist mit dem Netzwerk verbunden.
- Ein Benutzer hat sein Kennwort vergessen oder geändert. Es muss kein Challenge-Response-Verfahren durchgeführt werden, wenn der Client-Computer mit dem Netzwerk verbunden ist. Der Administrator kann das Windows-Kennwort zurücksetzen und der Benutzer kann sich über das AD in der Netzwerk-PBA anmelden. Bei einer erfolgreichen AD-Anmeldung findet ein Single Sign-On in Windows statt und die neuen Benutzeranmeldeinformationen werden zurück in die PBA synchronisiert.

Zur Konfiguration gehen Sie folgendermaßen vor (die Einstellungen auf den anderen Reitern entnehmen Sie bitte den jeweiligen Beschreibungen):

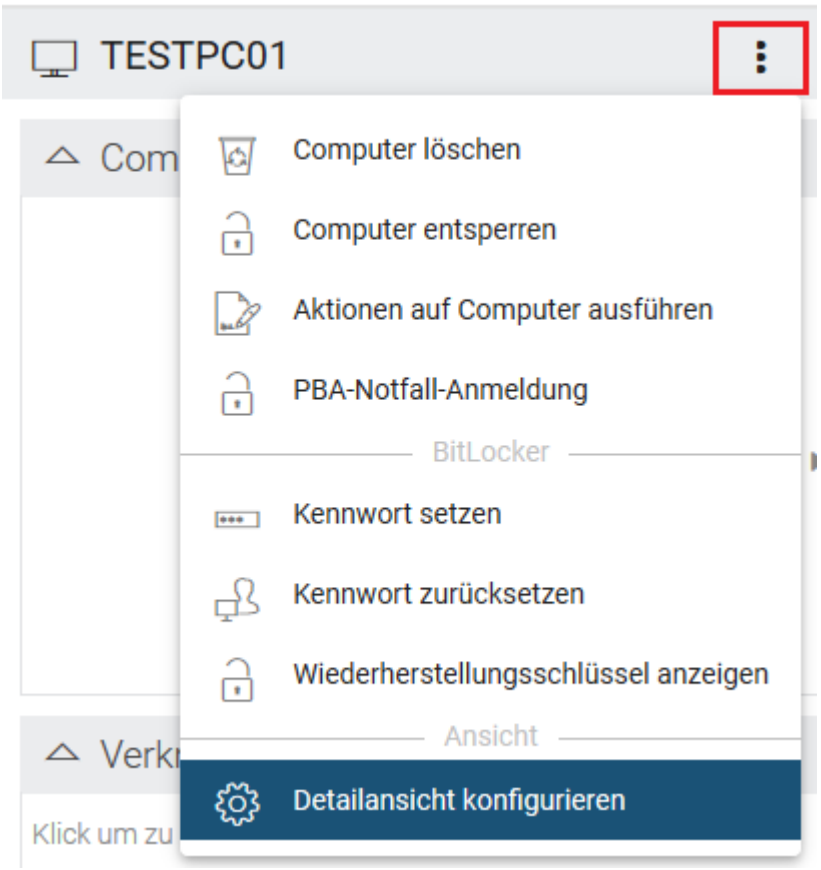


1. Wählen Sie die Grundeinstellung **Netzwerk-Pre-Boot-Authentifizierung aktivieren**.
2. Wählen Sie **Automatische Anmeldung am Netzwerk erlauben** aus.
3. Lassen Sie das Häkchen bei **Andere Anmeldemethoden zulassen** gesetzt.
4. Belassen Sie den Standardwert für die Ausfallsicherung bei 3. So können Sie sicherstellen, dass erst nach 3 erfolgreichen Netzwerk-Anmeldungen keine andere Möglichkeit mehr für eine Anmeldung besteht. Diese Option dient zum einen für Testzwecke und zum anderen als Ausfallsicherung.
5. Wählen Sie **Anmeldung über das Active Directory (AD) erlauben**.
6. Wählen Sie **Netzwerkanmeldung für alle AD-Benutzer erlauben**.
7. Je nachdem, ob eine Netzwerkanmeldung erzwungen werden soll oder nicht, wählen Sie die Option **Anmeldung von Benutzer muss ausschließlich über Netzwerk-Authentifizierung erfolgen** oder lassen Sie sie frei.
8. Belassen Sie den Standardwert 3 bei **Anzahl der automatischen Wiederholversuche bis Zustandekommen der Netzwerkverbindung**.
9. Ebenso können Sie die Pausen zwischen den Wiederholversuchen bei 5 Sekunden lassen.
10. Klicken Sie die Schaltfläche **Bestätigen**, um Ihre Eingaben zu übernehmen und schließen Sie den Dialog mit **OK**.

3.5.4 Netzwerk-PBA-Einstellungen im DOC

Gehen Sie folgendermaßen vor, um Einstellungen zur Netzwerk-Pre-Boot-Authentifzierung im DriveLock Operations Center vorzunehmen:

1. Wählen Sie den Bereich **Computer** und öffnen Sie das BitLocker-Dashboard.
2. Markieren Sie den DriveLock Agenten, dessen Einstellungen Sie ändern wollen.
3. Öffnen Sie in der Detailansicht auf der rechten Seite das Auswahlmenü, um die Detailansicht zu konfigurieren.



4. Wählen Sie aus der Liste **Netzwerk-Pre-Boot-Authentifizierung** und setzen Sie ein Häkchen bei **Anzeigen** und optional bei **Ausklappen** (je nachdem, ob Sie das Element gleich geöffnet anzeigen wollen).
5. Die Option **Automatische Anmeldung am Netzwerk erlauben** kann nur aktiviert oder deaktiviert werden.

Hinweis: Die Richtlinie mit dieser Einstellung muss dem DriveLock Agenten (Client-Computer) zugewiesen und dort ausgeführt worden sein.

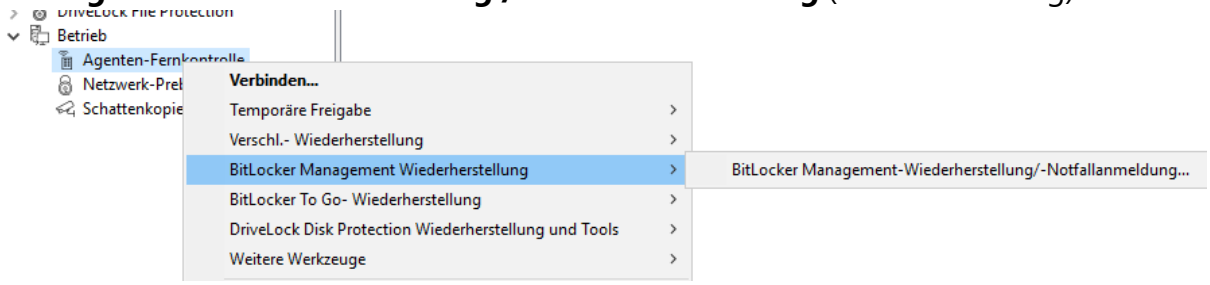
3.6 Einstellungen für die Notfall-Anmeldung

Wenn ein Benutzer nicht mehr in der Lage ist, sich an der Pre-Boot-Authentifizierung anzumelden (z.B. weil das Kennwort vergessen wurde), müssen Sie die Einstellungen für die Notfall-Anmeldung vornehmen.

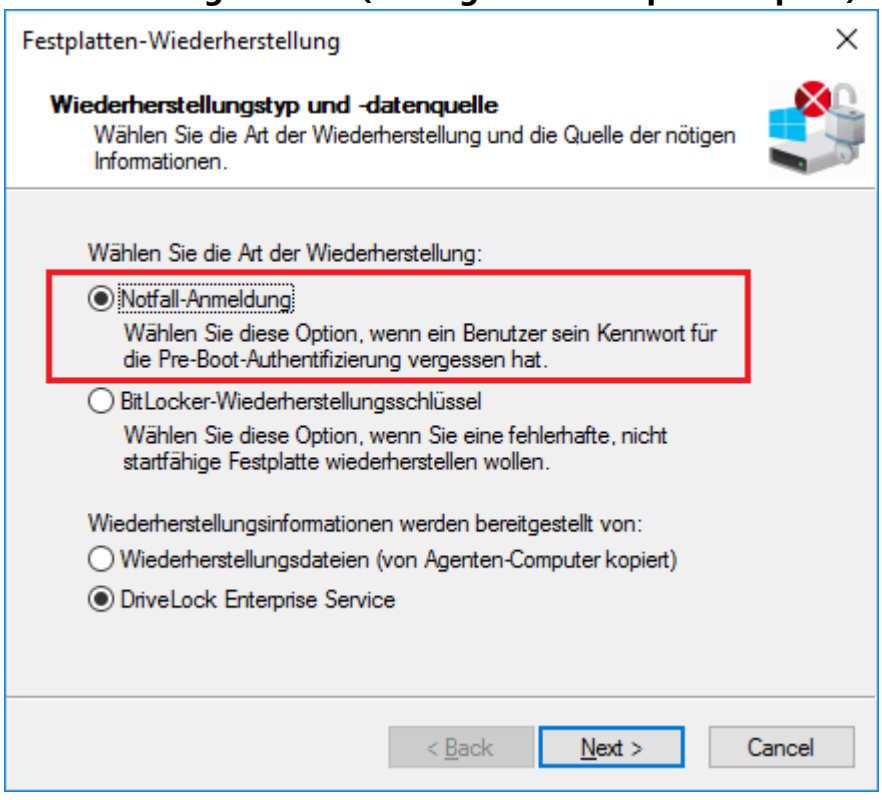
Hinweis: Weitere Informationen zur Interaktion zwischen Administrator und Endbenutzer finden Sie hier.

Gehen Sie folgendermaßen vor:

1. Um den Wiederherstellungs- bzw. Notfall-Assistenten zu starten, öffnen Sie die **DriveLock Management Konsole**, wählen im Knoten **Betrieb** den Unterknoten **Agenten-Fernkontrolle**, und öffnen durch Rechtsklick das Kontextmenü.
2. Hier wählen Sie **BitLocker Management Wiederherstellung** und dann **BitLocker Management-Wiederherstellung / Notfall-Anmeldung** (siehe Abbildung).



3. Der Wiederherstellungs-Assistent wird geöffnet.
   Wählen Sie auf der ersten Seite die Option **Notfall-Anmeldung**. Wenn Ihre Wiederherstellungs-Schlüssel zum DriveLock Enterprise Service gesendet werden, lassen Sie die Standardeinstellung **DriveLock Enterprise Service**. Wenn Sie den Pfad später zu den benötigten Wiederherstellungs-Schlüsseln angeben möchten, wählen Sie **Wiederherstellungsdateien (von Agenten-Computer kopiert)** aus.

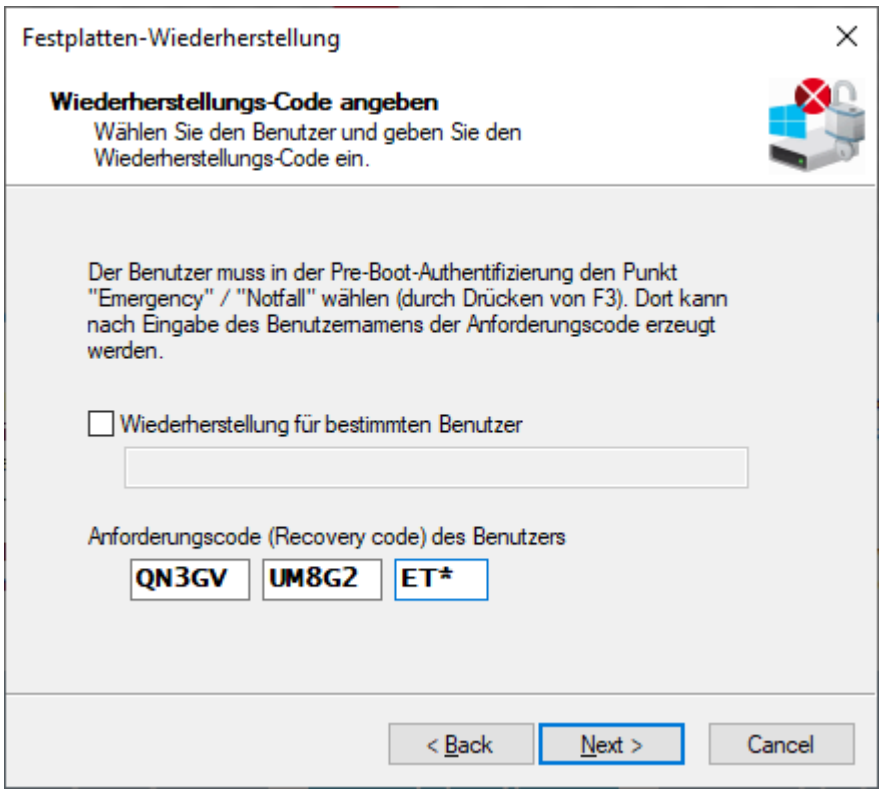


4. Für das Notfall-Anmeldeverfahren benötigen Sie den privaten Schlüssel des Wiederherstellungs-Zertifikates. Im zweiten Dialog geben Sie den Speicherort an, entweder Windows-Zertifikatsstore, eine Smartcard oder eine PFX-Datei zusammen mit

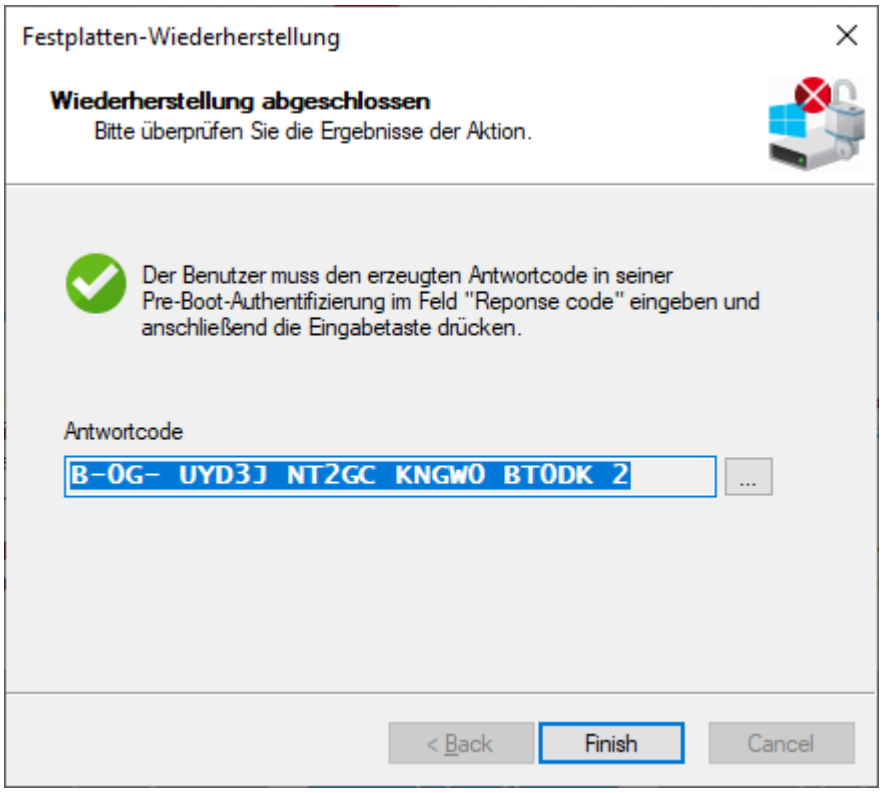
dem jeweiligen Kennwort. Weitere Informationen zu Zertifikaten finden Sie hier. Klicken Sie **Weiter**.

5. Im dritten Dialog wird eine Liste der Computer angezeigt, aus der Sie den wiederherzustellenden Computer auswählen. Setzen Sie ein Häkchen bei der Option **nur den neuesten Eintrag pro Computer zeigen**. Klicken Sie **Weiter**.
6. Als nächstes erscheint die Seite zur Eingabe des Anforderungs- bzw. Wiederherstellungscodes des Benutzers.
   Geben Sie den Code in die entsprechenden Felder ein (siehe Abbildung). Sie können optional den Namen des Benutzers angeben.

> Achtung: Zwingend erforderlich ist jetzt der Wiederherstellungscode, den Ihnen der Benutzer übermitteln muss.



7. Klicken Sie **Weiter**, um den Antwortcode generieren zu lassen.



8. Teilen Sie dem Benutzer der **Antwortcode** mit.
9. Klicken Sie **Fertigstellen**.

3.7 DriveLock Agent

3.7.1 Installation der DriveLock-PBA auf dem DriveLock Agenten

Bitte beachten Sie folgendes:

1. Nach dem Start des Client-Computers erscheint ein Hinweis, dass die DriveLock PBA installiert wird.
2. Nach der Bestätigung wird der Rechner neu gestartet.

> Hinweis: Wenn kein Benutzer angemeldet ist, wird der Rechner sofort neu gestartet

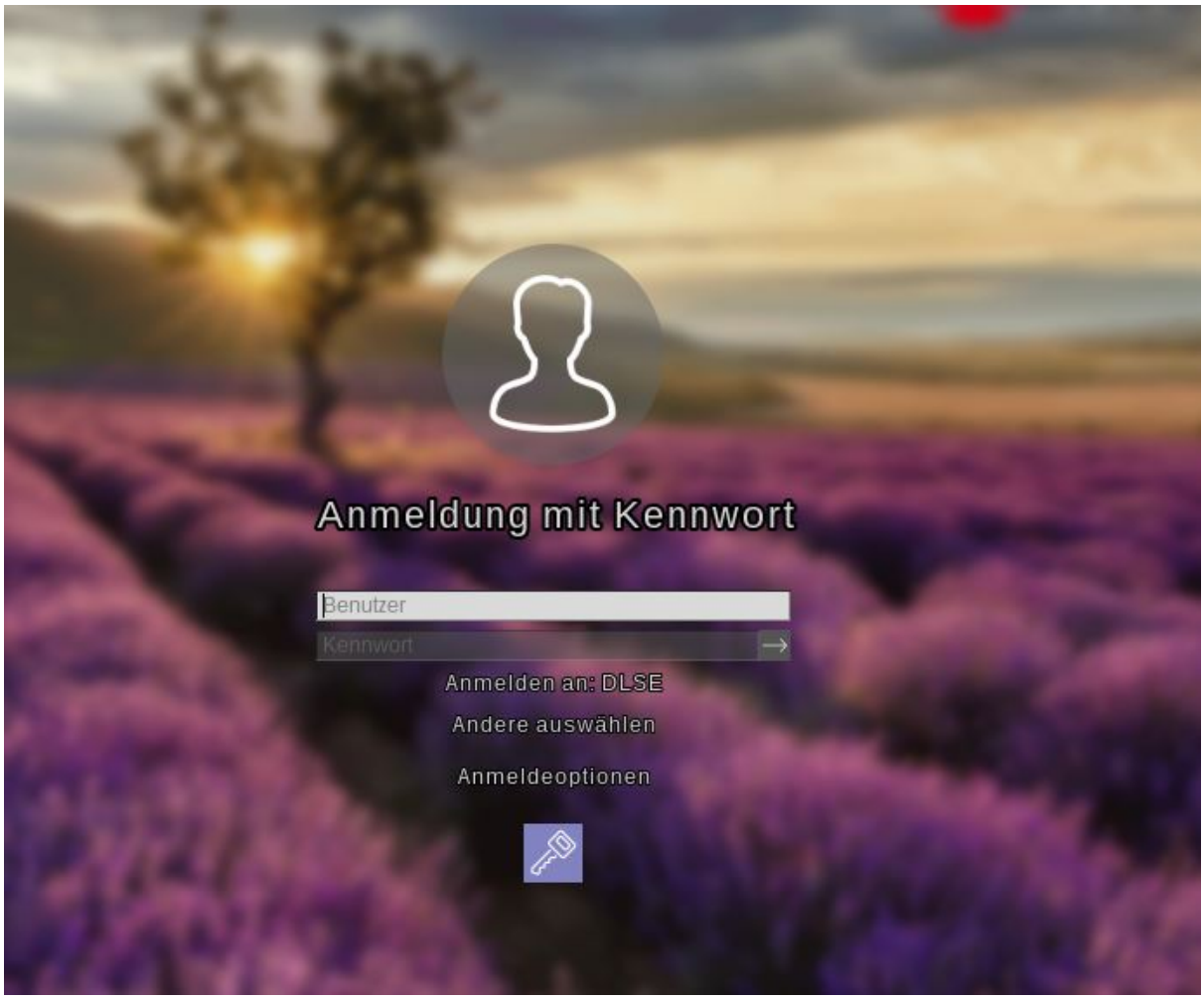
3. Nach dem Neustart des Client-Computers und nach der Anmeldung erscheint ein weiterer Dialog (siehe Abbildung), der darüber informiert, dass ab jetzt die DriveLock-PBA aktiv ist.

4. Gleichzeitig wird die Verschlüsselung gestartet, ein Neustart oder ein Herunterfahren des Rechners ist von nun an jederzeit möglich.

3.7.2 Anmeldung an der DriveLock-PBA

Bei der Anmeldung ist folgendes zu beachten:

1. Sobald der Client-Computer gestartet wird, wird ein Kurztext angezeigt, dass die DriveLock Pre-Boot Authentifizierung aktiv ist.
2. Sofort nach der Textanzeige und noch vor Anzeige des Startbildschirms können Abkürzungstasten ('Hot Keys') verwendet werden.
3. Durch Drücken einer beliebigen Taste oder einem Mausklick wird die Anmeldeseite angezeigt.



Die Verwendung von Funktionstasten ist nicht mehr notwendig, aber möglich.

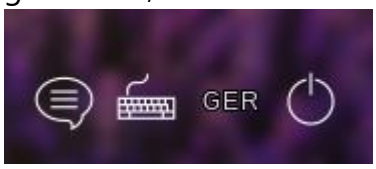
4. Auf der Anmeldeseite müssen die Windows-Anmeldedaten angegeben werden.

> Achtung: Aus Sicherheitsgründen wird der zuletzt angemeldete Benutzer nicht gespeichert bzw. angezeigt.

Bitte beachten Sie folgendes:

- Der Benutzer muss sich zuvor an Windows angemeldet haben, wenn Sie die Option "Windows Benutzer automatisch synchronisieren" ausgewählt haben. Weitere Informationen finden Sie im Kapitel Benutzersynchronisation.
- Sie können Benutzer über eine Richtlinien-Einstellung auch zuvor bereits aus dem Active Directory importieren. Weitere Informationen finden Sie im Kapitel Benutzer.
- Kennwörter dürfen nur ASCII-128-Zeichen enthalten, damit die Authentifizierung in der PBA erfolgreich sein kann

5. Klicken Sie **Andere auswählen**, um die Domäne auszuwählen. Die verfügbaren Domänen werden angezeigt.
6. Wenn keine Tastatur vorhanden ist (z.B. auf einem Tablet-Computer), kann über das **Tastatursymbol** unten rechts eine Bildschirmtastatur eingeblendet werden.
   Am Tastatursymbol wird ein grünes Häkchen angezeigt. Die Tastatur wird eingeblendet, wobei der Fokus in einem Textfeld stehen muss.

   Über das Sprechblasensymbol lässt sich die Sprache der Anmeldeoberfläche einstellen.
7. Alle Felder und Optionen können auch mit <Tab>, <Shift-Tab> und den Pfeiltasten erreicht werden, sofern keine Maus vorhanden ist.
8. Über die Auswahl der Sprache (in der Abbildung **GER**) unten rechts besteht die Möglichkeit, ein anderes Tastaturlayout auszuwählen.
9. Die Anmeldung erfolgt entweder durch Klicken der Pfeiltaste neben dem Kennwort oder durch Drücken der Return-Taste.
10. In der Standardeinstellung wird der Benutzer anschließend auch an Windows angemeldet (Single Sign On). Dieses Verhalten kann in der Richtlinie deaktiviert werden.

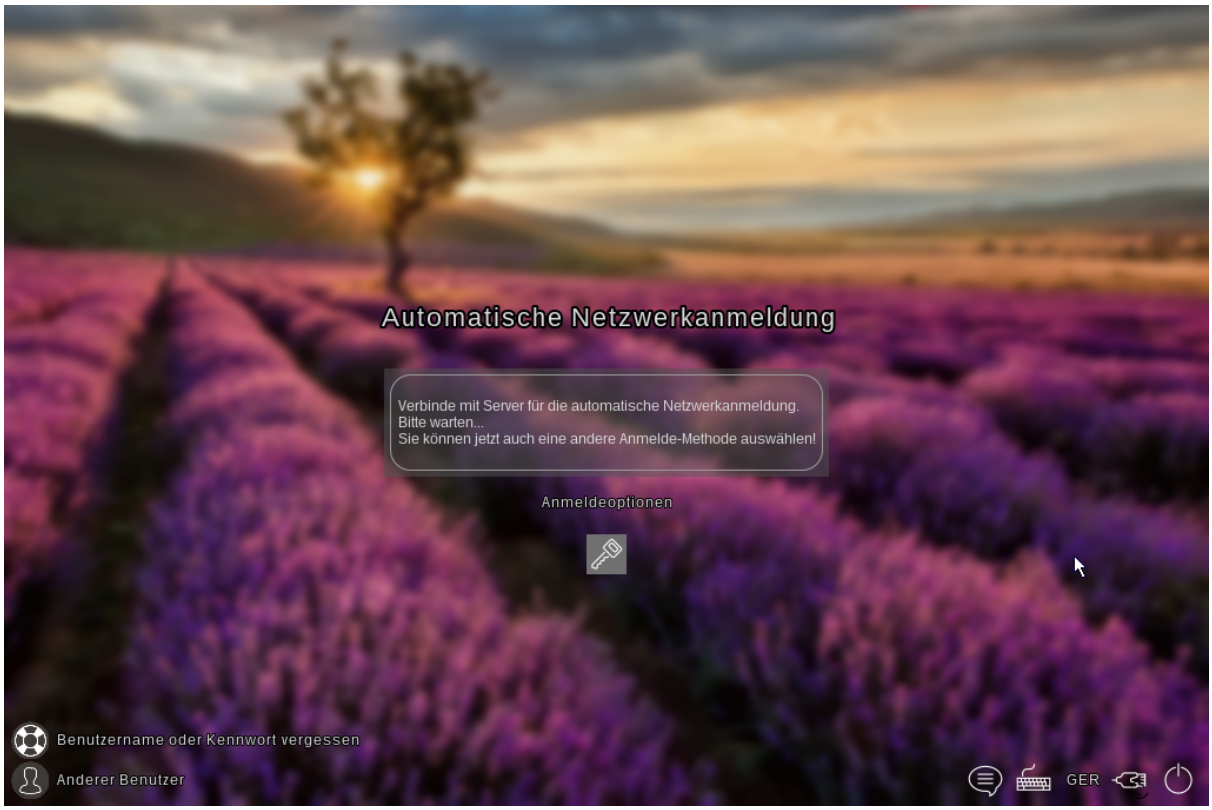
3.7.3 Netzwerk-Preboot-Authentifizierung

Wenn die Richtlinie mit den Netzwerk-PBA-Einstellungen auf dem Client-Computer zugewiesen ist und dieser anschließend gestartet wird, kommen folgende Szenarien in Betracht:

1. **Der Client-Computer ist mit dem Unternehmensnetzwerk verbunden**

   Beim Hochfahren des Client-Computers wird ein Kurztext angezeigt, dass die DriveLock Pre-Boot Authentifizierung aktiv ist.
   Dann erscheint folgender Anmeldebildschirm, siehe Abbildung:

   Hinweis: Eine Benutzerinteraktion ist nicht erforderlich.

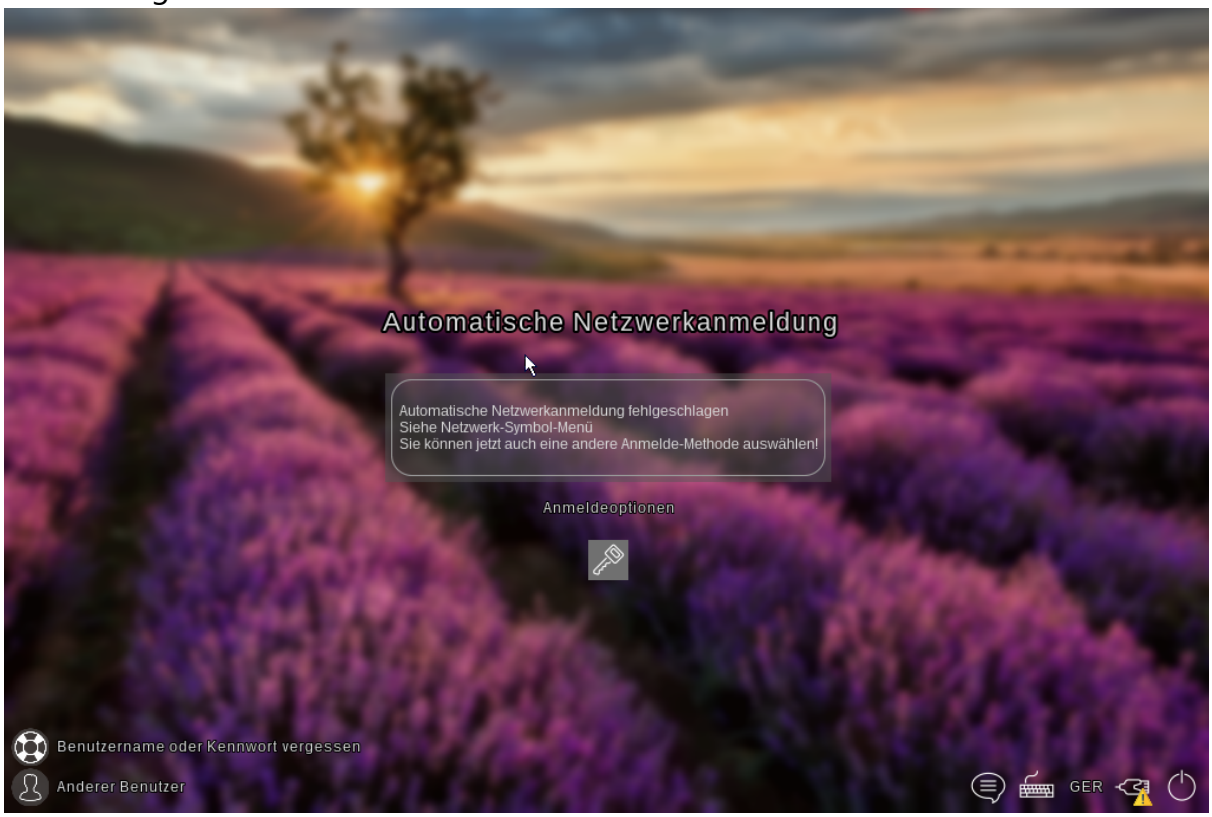


   Hinweis: Durch Anklicken des Schlüssel-Symbols innerhalb von 10 Sekunden kann, sofern erlaubt, zur Anmeldung an der PBA mit Eingabe von Benutzername- und Kennworteingabe umgeschaltet werden.

   Im nächsten Schritt wird die Windows-Anmeldemaske angezeigt, in der die Windows-Anmeldeinformationen eingegeben werden.

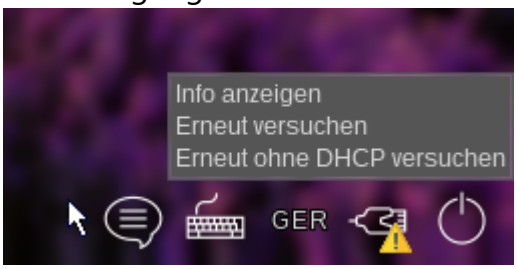
2. **Der Client-Computer kann sich nicht mit dem Unternehmensnetzwerk verbinden**

   Beim Hochfahren des Client-Computers wird ebenfalls der Kurztext angezeigt, dass die DriveLock Pre-Boot Authentifizierung aktiv ist. Der Anmeldebildschirm zeigt jetzt allerdings an, dass die automatische Netzwerkanmeldung fehlgeschlagen ist. Je nach Einstellung in der Richtlinie wird das System einige Male versuchen, automatisch eine Verbindung herzustellen.



Wenn keine Verbindung hergestellt werden kann, hat der Benutzer je nach Einstellung in der Richtlinie folgende Möglichkeiten:

- Versuchen, die Netzwerkverbindung erneut herzustellen
  Über das **Netzwerk-Symbol-Menü** in der Taskleiste stehen folgende Optionen zur Verfügung:



- Sofern erlaubt, eine andere Anmelde-Methode wählen (Benutzername-/Kennworteingabe). In diesem Fall ist Single Sign-On aktiv und die Anmeldung muss nur einmal an der DriveLock PBA erfolgen.

> Achtung: Wenn keine andere Anmelde-Methode erlaubt ist, ist es ohne Netzwerkverbindung nicht möglich, das Betriebssystem des Client-Computers zu starten.

> Hinweis: Weitere Informationen, u.a. zur Verwendung von Abkürzungs- und Funktionstasten, finden Sie im Kapitel Anmeldung an der DriveLock-PBA.

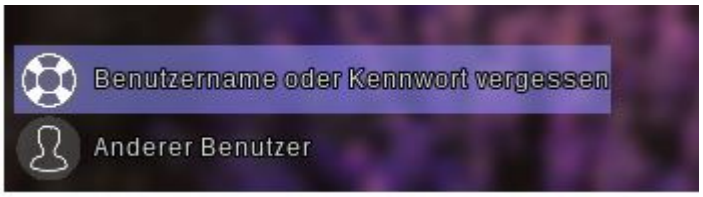
3.7.4 Notfall-Anmeldung mit Wiederherstellungscode

Szenario: Der Benutzer eines DriveLock Agenten hat sein Kennwort vergessen und kann sich nicht an der DriveLock PBA authentifizieren. Er fordert Unterstützung beim Administrator an.

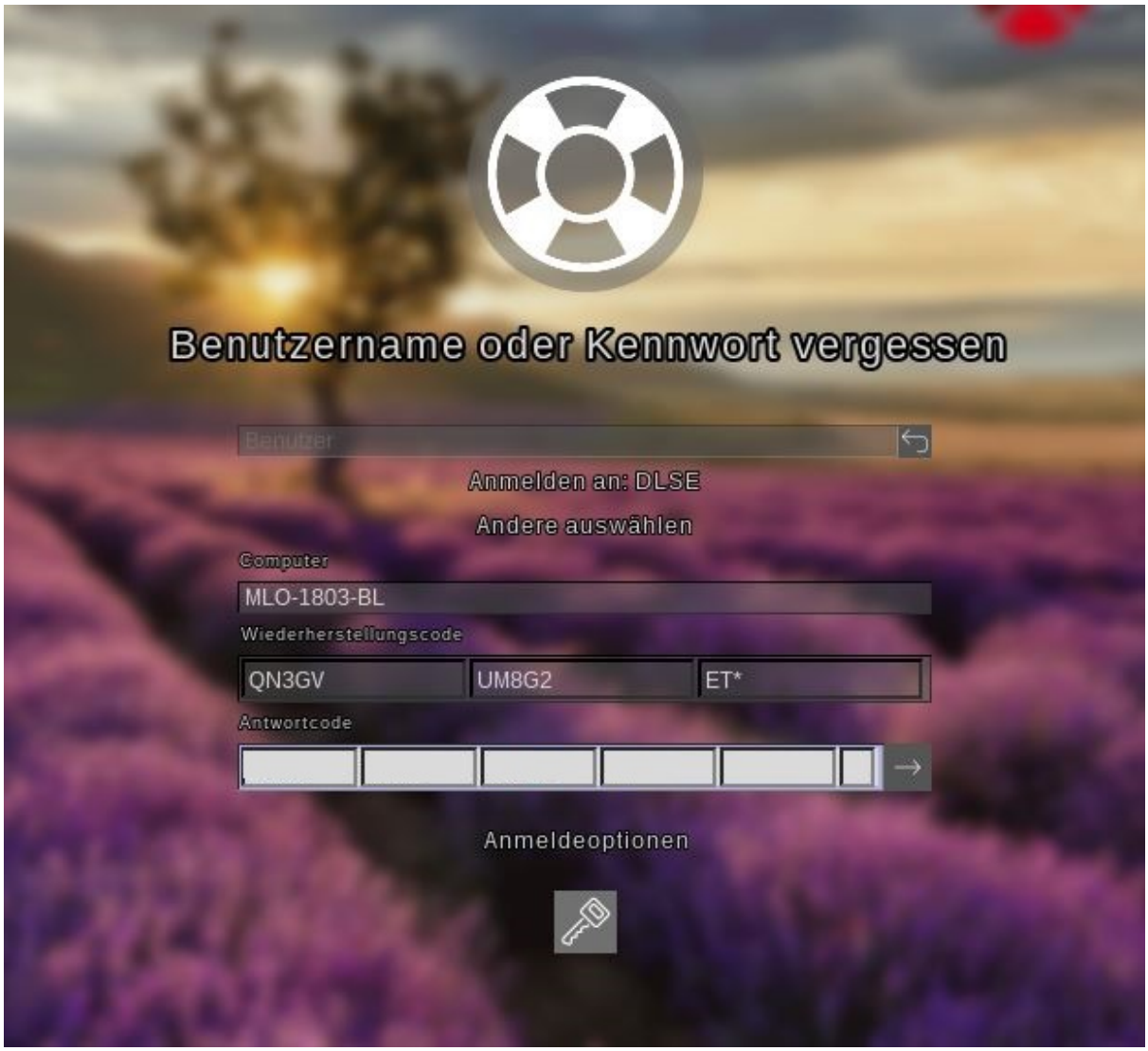
Benutzer und Administrator führen nun folgende Aktionen durch:

1. Benutzeraktion:

1. Wählen Sie die Option **Benutzername oder Kennwort vergessen** auf der linken Seite des Anmeldebildschirms aus.



2. Anschließend erscheint ein neuer Anmeldebildschirm, in dem Ihr Anforderungs- bzw. Wiederherstellungscode angezeigt wird.



3. Teilen Sie den Wiederherstellungscode und Maschinenname dem Administrator mit, ggf. auch den Benutzernamen.

> Hinweis: Während der Benutzername optional ist, müssen Maschinenname und Wiederherstellungscode unbedingt angegeben werden.

2. Administratoraktion:

1. Sie haben nach Mitteilung des Benutzers sofort den Wiederherstellungs-Assistenten aufgerufen und nun die Eingabemaske für den Anforderungs- bzw. Wiederherstellungscode erreicht.
2. Geben Sie den **Anforderungscode** ein und generieren Sie dadurch den **Antwortcode**.
3. Teilen Sie den **Antwortcode** nun dem Benutzer mit.

Achtung: Sowohl der Anforderungs- als auch der Antwortcode werden einmalig generiert und können nur einmalig verwendet werden.

3. Benutzeraktion:

1. Geben Sie den **Antwortcode** in die entsprechenden Felder in der DriveLock PBA ein. Wenn Sie einen Fehler bei der Eingabe machen, bekommen Sie verschiedenfarbige Fehlerziffern angezeigt.
   Wenn Sie alles korrekt eingegeben haben, können Sie sich durch Klicken auf die Pfeiltaste wieder am System anmelden.

2. Melden Sie sich selbst bei Windows an.

Achtung: Single Sign-On ist jetzt nicht aktiv!

3.7.5 Windows-Authentifizierung

Jedes Mal wenn sich ein Benutzer erfolgreich manuell an Windows anmeldet, wird das jeweils aktuellste Windows-Kennwort der Pre-Boot-Benutzerdatenbank hinzugefügt. Das gleiche passiert, wenn ein Benutzer sein persönliches Kennwort unter Windows ändert.

Das Verhalten der Anmeldung hängt von der Einstellung in der DriveLock Richtlinie ab: ·

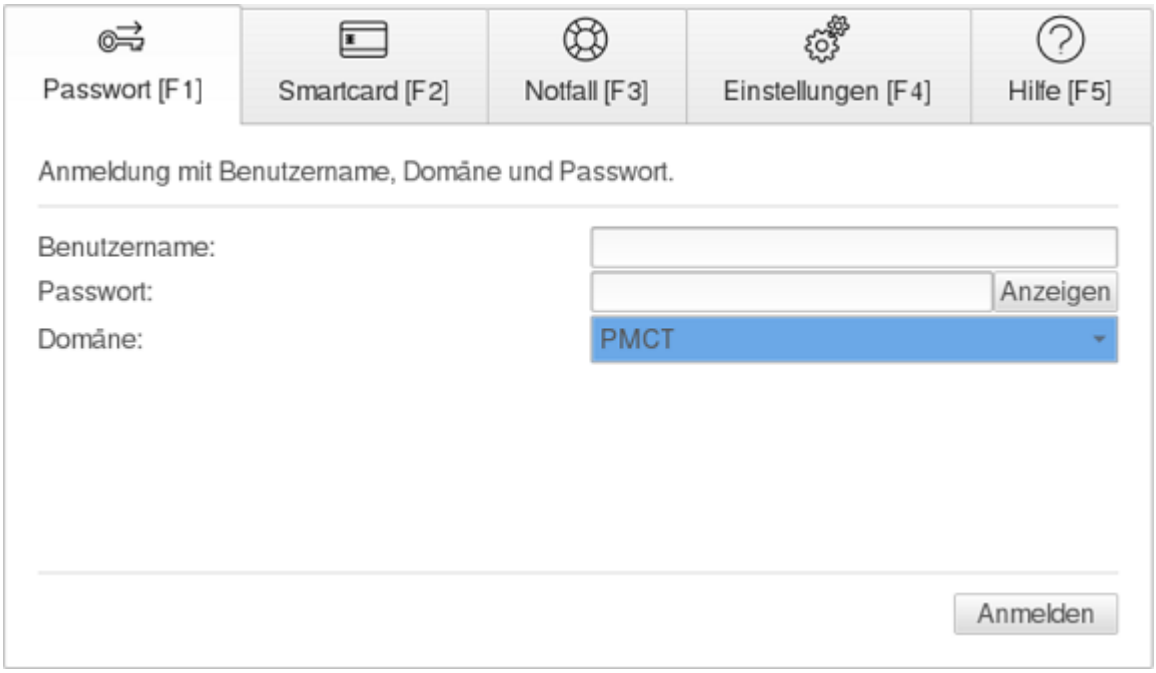
- Automatisch: **Single Sign-On Modus** ist eingeschaltet: der Benutzer wird automatisch bei Windows angemeldet.
- Manuell: **Single Sign-On Modus** ist ausgeschaltet: der Windows-Anmelde-Bildschirm angezeigt und der Benutzer muss sich mit seinen persönlichen Anmeldeinformationen anmelden.

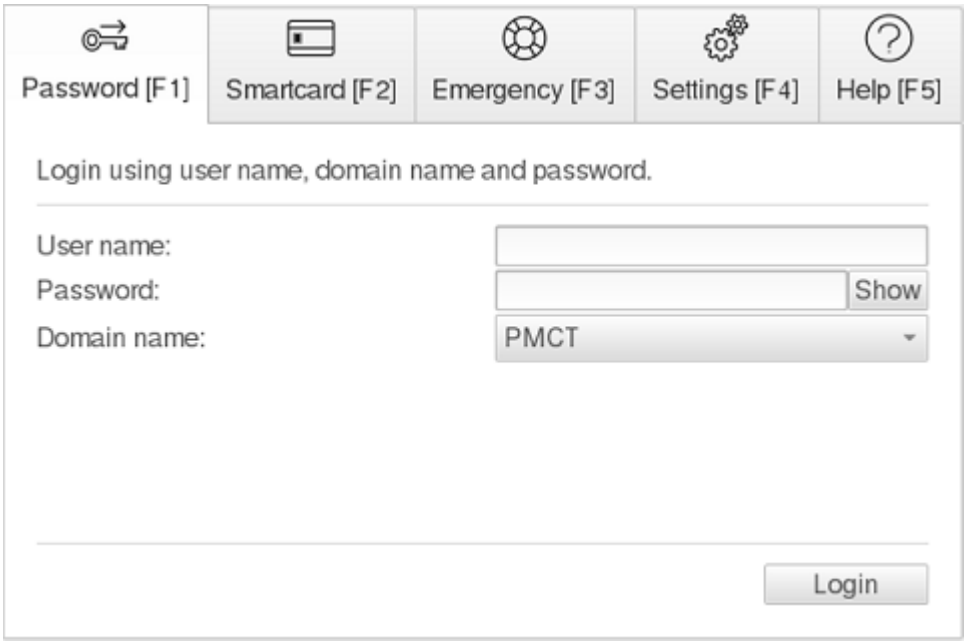
3.7.6 BIOS Pre-Boot-Authentifizierung

Wenn die Disk Protection PBA auf einem Legacy-BIOS System installiert wurde, wird die Authentifizierung folgendermaßen ablaufen.

Authentifizierung mit Benutzername, Kennwort und Domänenname

Wenn in den Einstellungen für die Pre-Boot-Authentifizierung entweder die Authentifizierungs-Methoden **Lokale Anmeldung** oder **Domänenbenutzer (mit Kennwort)** aktiviert sind, zeigt DriveLock Disk Protection den folgenden Bildschirm an:





Wenn beide Authentifizierungs-Optionen Lokale Anmeldung und/oder Domänenbenutzer (mit Kennwort) aktiviert sind, wird durch Drücken der Funktionstaste F2 zum Smartcard-Anmeldebildschirm umgeschaltet.

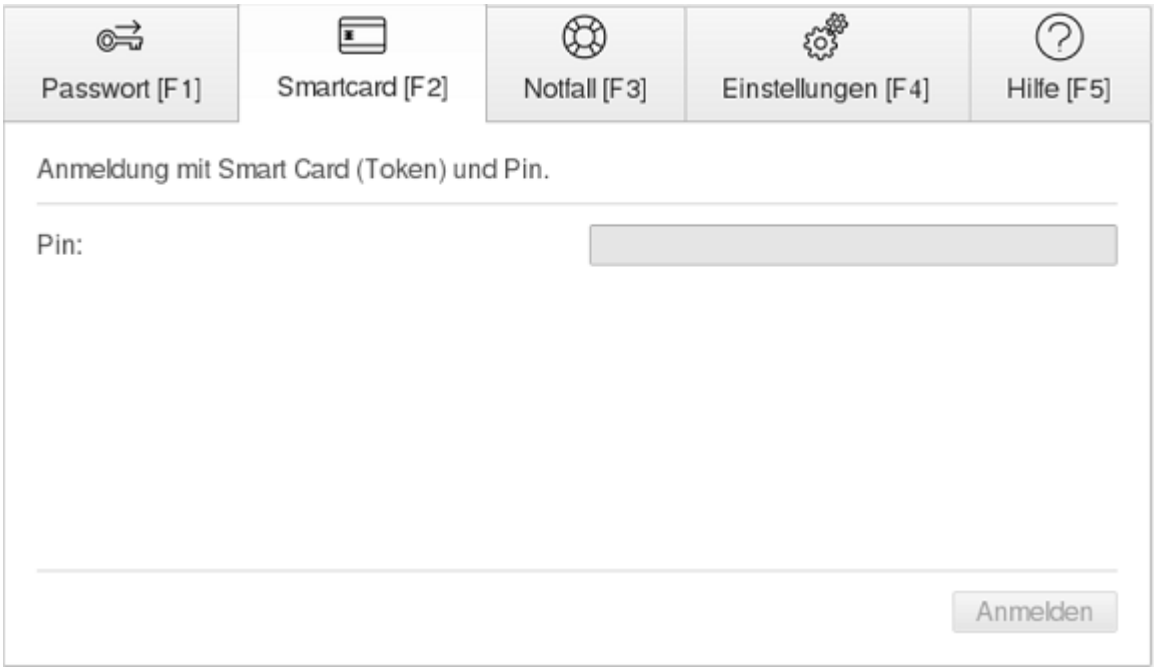
Das Feld **Domäne** enthält alle relevanten Domänen, wenn Domänenbenutzer (mit Kennwort) Option ausgewählt wurde. Der lokale Systemname kann ebenfalls in diesem Feld eingetragen sein. Benutzen Sie den [Pfeil-hoch] und [Pfeil-runter] um durch die Liste der verfügbaren Domänennamen zu blättern.

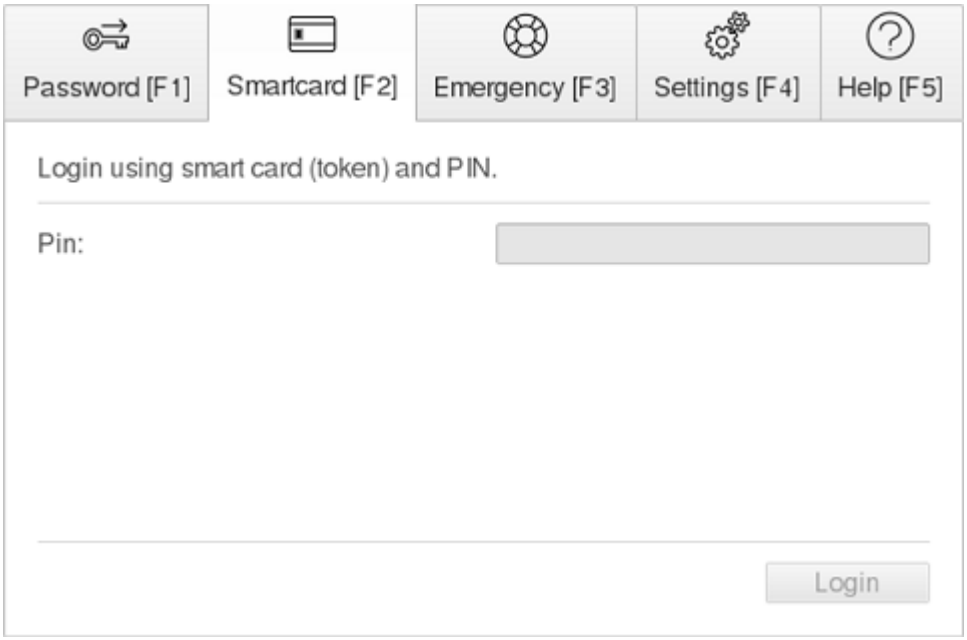
Hinweis: Beachten Sie, dass im Fall von aufeinanderfolgenden fehlerhaften Pre-Boot-Authentifizierungsversuchen die Sperr-Richtlinie erzwungen wird, um ein Erraten des Kennwortes zu verhindern. Öffnen Sie unter Windows das Ereignisprotokoll des Systems, um weitere Details zu den fehlerhaften Login-Versuchen und anderen Ereignissen zu entnehmen.

Wenn der Benutzer sich nicht mehr an dem System anmelden kann (z.B. er erinnert sich nicht an das korrekte Kennwort), kann das Notfall Anmeldeverfahren mit Benutzername gestartet werden.

Authentifizierung mit Smartcard/Token und PIN

Wenn die Disk Protection Authentifizierungs-Methoden **Domänenbenutzer (mit Token)** oder Zugriff mit Shared Key aktiviert sind, dann sieht das Pre-Boot-Authentifizierungs-Fenster wie unten abgebildet aus:





Wenn beide Authentifizierungs-Optionen Lokale Anmeldung und/oder Domänenbenutzer (mit Kennwort) aktiviert sind, wird durch Drücken der Funktionstaste F1 zum Benutzernamen/Passwort/Domänennamen Bildschirm umgeschaltet.

An diesem Punkt kann sich der Benutzer mit seiner Smartcard/Token und PIN am System authentifizieren. Bitte beachten Sie, dass in dem Fall von aufeinanderfolgenden fehlerhaften Pre-Boot Authentifizierungsversuchen die Sperr-Richtlinie erzwungen wird, um ein Erraten der PIN zu verhindern (Öffnen Sie das Ereignisprotokoll des Systems, um weitere Details zu den fehlerhaften Login-Versuchen und anderen Ereignissen zu entnehmen).

Wenn der Benutzer sich nicht an seine korrekte PIN erinnert und sich deshalb nicht am System anmelden kann, kann das Notfall Anmeldeverfahren für Token Benutzer gestartet werden.

3.8 DriveLock-PBA-Kommandozeilenprogramm

Administratoren können das Kommandozeilenprogramm `DLFDEcmd` sowohl bei Verwendung der DriveLock-PBA für BitLocker als auch für DriveLock Disk Protection (Full Disk Encryption, FDE) einsetzen. Setzen Sie das Tool ein, um sich beispielsweise den Status der PBA anzeigen zu lassen oder um eine automatische Anmeldung (Autologon) am Client-Computer zu initiieren, wenn Windows-Systemupdates erforderlich werden.

> Hinweis: Je nach gewählter Verschlüsselungstechnologie (Disk Protection - FDE oder BitLocker Management) wird der Anzeigetext entsprechend angepasst.

Englische Hilfe zur Verwendung der einzelnen Befehle wird angezeigt, wenn Sie das Programm `DLFdeCmd.exe` mit dem Parameter 'help' aufrufen.

Nachfolgend die detaillierte Beschreibung der einzelnen Parameter:

- `SHOWSTATUS`: Zeigt den aktuellen Status der verwendeten Verschlüsselungstechnologie an.
- `CRYPTSTATUS`: Zeigt Informationen zum aktuellen Verschlüsselungsstatus an, z.B. die Anzahl der verschlüsselten Festplatten.
- `ENABLEAUTOLOGON`: Aktiviert die automatische Anmeldung im Rahmen der Festplattenverschlüsselung für die nächste Anzahl von Anmeldungen.
  Hierbei geben Sie folgendes an:
  - `<user>`: PBA-Benutzer zur automatischen Anmeldung
  - `<domain>`: Domäne des angegebenen PBA-Benutzers
  - `<password>`: Kennwort des angegebenen PBA-Benutzers (* zur Eingabe des Kennworts, # zur Eingabe in einem Dialog)
  - `<count>`: Anzahl der Neustarts, bei denen die automatische Anmeldung aktiv sein sollte. Geben Sie 'forever' an, wenn die automatische Anmeldung auf unbestimmte Zeit aktiviert werden soll.
  - `[sso]` : Fügen Sie "sso" nur hinzu, wenn die automatische Anmeldung mit Single Sign On erfolgen soll.

Beispiel: Bei Eingabe von `enableautologon hans dlse * 2` wird Benutzer 'hans' aus der Domäne 'dlse' bei den nächsten '2' Neustarts automatisch angemeldet, das Kennwort wird in der Kommandozeile eingegeben.

> Hinweis: Für die automatische Anmeldung mit einer Smartcard oder einem Token geben Sie "token" für `<user>` und `<domain>` an.

- `DISABLEAUTOLOGON`: Deaktiviert die automatische Anmeldung
- `SHOWAUTOLOGON`: Zeigt die Einstellungen für die automatische Anmeldung
- `ENABLERESETSP`: Aktiviert das Zurücksetzen der Systemschutz-Interruptvektorliste nach dem nächsten Neustart. Diese Option sollte nach einem Update des System-BIOS verwendet werden, um neue Interruptvektorwerte zu speichern und die PBA-Warnmeldungen zu unterdrücken. Eine einmalige automatische Anmeldung ist erforderlich, um die Interruptvektorliste zurückzusetzen.
  Auch hier sind Angaben unter `<user> <domain> <password>` erforderlich.
- `DISABLERESETSP`: Deaktiviert das Zurücksetzen des Systemschutz-Interruptvektors
- `SHOWRESETSP`: Zeigt die aktuellen Einstellungen zum Zurücksetzen des Systemschutzes an
- `ENABLEDELAYINST`: Verzögert die Installation der Festplattenverschlüsselung, bis "DisableDelayInst" ausgeführt wurde.
- `DISABLEDELAYINST`: Deaktiviert die Verzögerung und führt die Installation der Festplattenverschlüsselung aus, wie in der Richtlinie konfiguriert
- `SHOWDELAYINST`: Zeigt den aktuellen Status der verzögerten Installation an

In der Abbildung unten ist das Autologon für BitLocker Management deaktiviert, der Befehl `ENABLEAUTOLOGON` wurde in diesem Fall nicht gesetzt.

```
C:\WINDOWS\system32>DlFdeCmd SHOWAUTOLOGON
------------------------------------------------------------------------
DriveLock 19.2.0 : Data protection, encryption, and more
DLFdeCmd         : Full disk encryption command line tool
                   (C) Copyright 2004-2019 DriveLock SE.
------------------------------------------------------------------------

BitLocker Management auto-logon is currently disabled.

C:\WINDOWS\system32>DlFdeCmd SHOWRESETSP
------------------------------------------------------------------------
DriveLock 19.2.0 : Data protection, encryption, and more
DLFdeCmd         : Full disk encryption command line tool
                   (C) Copyright 2004-2019 DriveLock SE.
------------------------------------------------------------------------

BitLocker Management system protection reset is not active.

C:\WINDOWS\system32>DlFdeCmd SHOWDELAYINST
------------------------------------------------------------------------
DriveLock 19.2.0 : Data protection, encryption, and more
DLFdeCmd         : Full disk encryption command line tool
                   (C) Copyright 2004-2019 DriveLock SE.
------------------------------------------------------------------------

BitLocker Management installation will execute as configured.

C:\WINDOWS\system32>
```

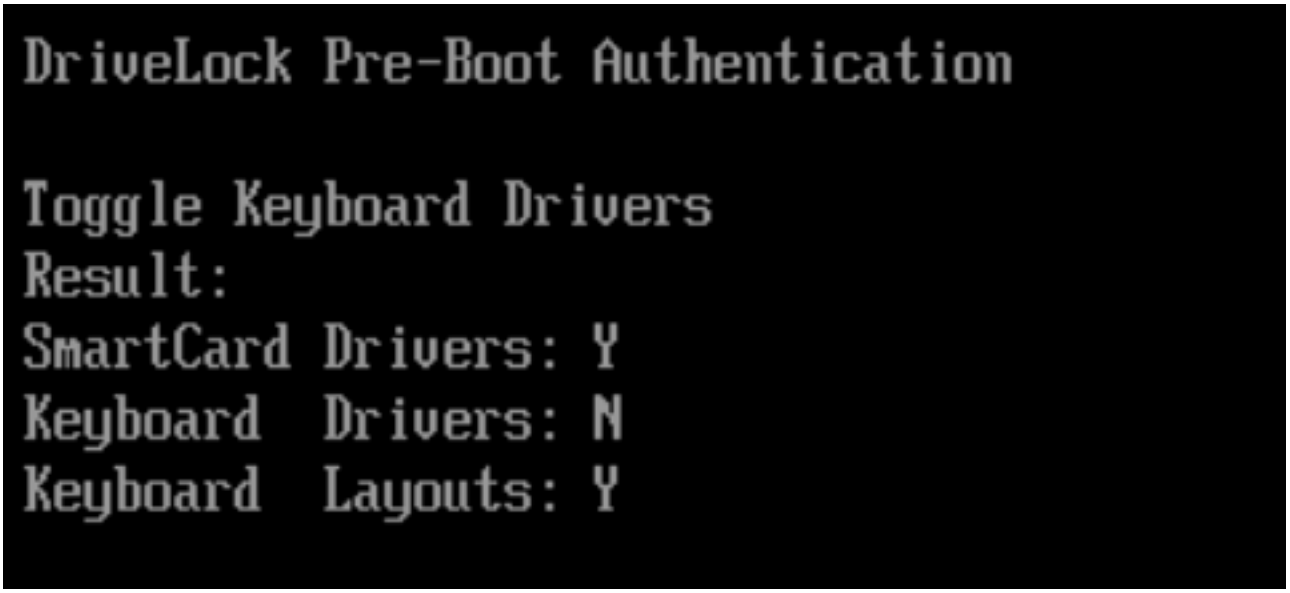
3.9 Abkürzungs- und Funktionstasten

Bei Bedarf können durch die Verwendung von Abkürzungstasten die Einstellungen für das Laden bestimmter Treiber umgekehrt werden, um Probleme beim Start der PBA auf bestimmten Systemen zu vermeiden.

Taste	Funktion (mit Standardeinstellungen)
k	Keyboard-Treiber werden nicht geladen
l	In der PBA stehen keine Tastatur-Layouts außer des Standardlayouts der Firmware zur Verfügung
s	Keine Smartcard Unterstützung

Taste	Funktion (mit Standardeinstellungen)
a	Alle oben genannten Funktionen werden ausgewählt
b	Umschalten von Keyboard-Treibern und Layouts (b->both)
c	Umschalten zwischen den Keyboard- bzw. Kombi-Treibern (c->combi)

Danach wird der aktuelle Status vor dem Laden der PBA kurz angezeigt (siehe Beispiel in Abbildung unten).



Hinweis: Der Kombi-Treiber kombiniert sowohl PS/2-Keyboard als auch PS/2-Maus in einem Treiber, um eine Fehlkommunikation zwischen den Treibern zu vermeiden.

Folgende Funktionstasten können innerhalb des Startbildschirms verwendet werden:

Taste	Funktion
F1	Anmeldung mit Kennwort
F2	Anmeldung mit Token

Taste	Funktion
F3	Notfall-Anmeldung
F5	Hilfe-Aufruf
F8	Forcierte Prüfung auf Token

4 DriveLock BitLocker To Go

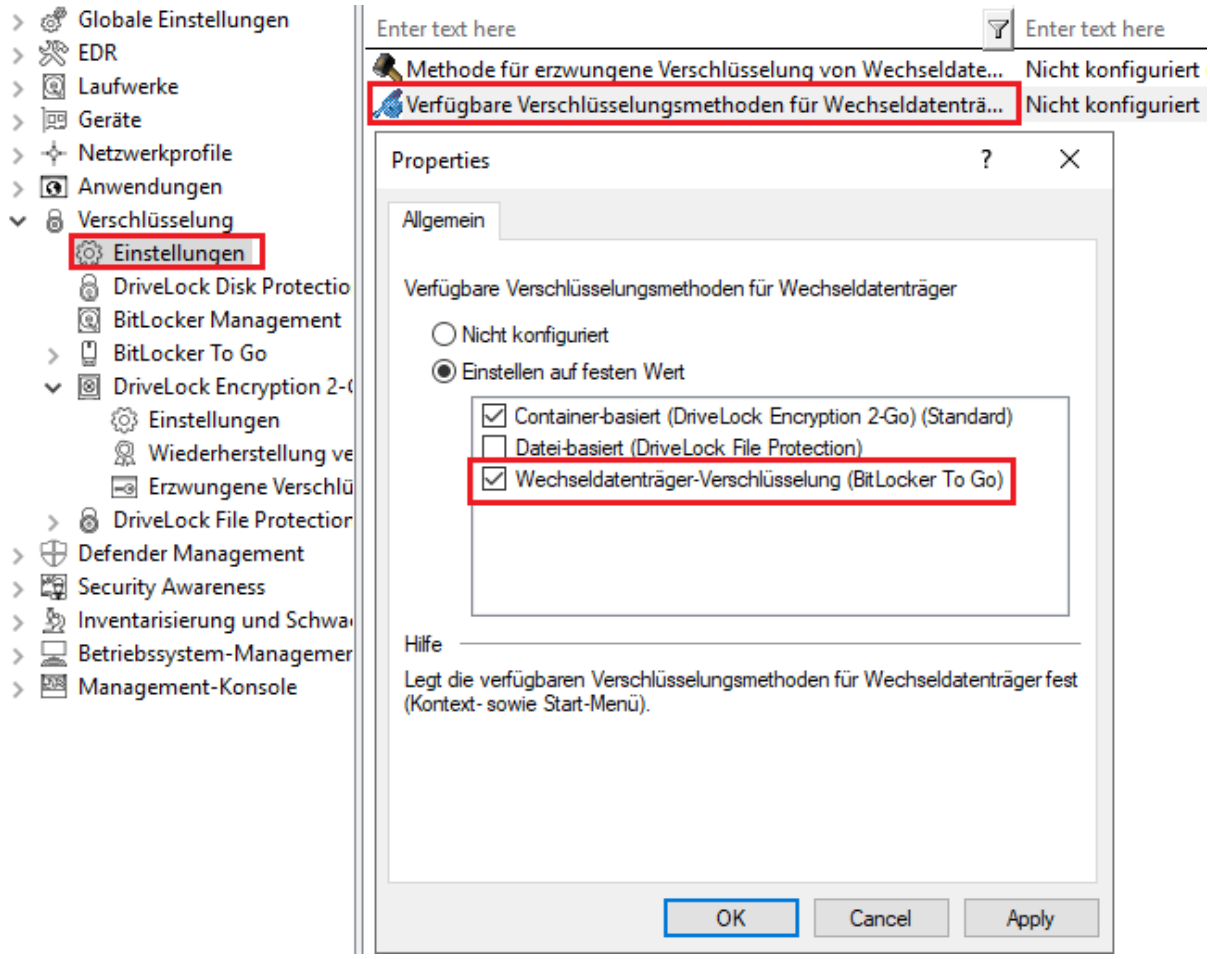
DriveLock BitLocker To Go bietet Ihnen folgende Funktionalitäten:

- Erzwungene Verschlüsselung von externen USB-Speichermedien mit BitLocker To Go
- Erzwungene Verschlüsselung von externen Laufwerken (z.B. eSATA-Festplatten)
- DriveLock erkennt bereits mit BitLocker To Go verschlüsselte USB-Laufwerke und verschlüsselt sie während der erzwungenen Verschlüsselung nicht erneut
- Benutzer können ein Kennwort eingeben
- Ein einheitliches Unternehmenskennwort kann vergeben werden, wodurch erzwungen wird, dass auf Daten nur innerhalb eines Unternehmens zugegriffen werden kann
- Wiederherstellung verschlüsselter Daten ist wie gewohnt möglich
- Verwaltung von zentraler Stelle aus

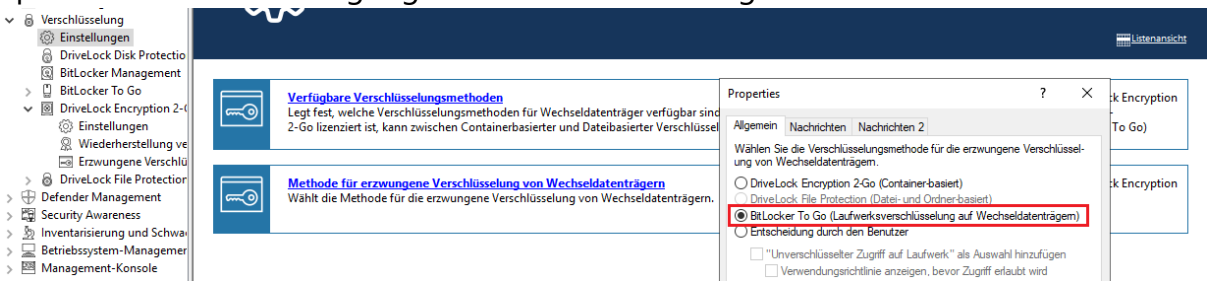
4.1 Voraussetzungen für BitLocker To Go

Damit Sie BitLocker To Go für die Verschlüsselung von externen USB-Speichermedien oder Laufwerken einsetzen können, müssen zwei Voraussetzungen erfüllt sein:

1. Sie haben eine gültige Lizenz für das Produkt.
2. Sie wählen als Verschlüsselungsmethode unter den allgemeinen Einstellungen für die Verschlüsselung BitLocker To Go aus.
   Gehen Sie vor, wie in der Abbildung gezeigt.
   Unter **Verfügbare Verschlüsselungsmethoden für Wechseldatenträger** wählen Sie die Option **Wechseldatenträger-Verschlüsselung (BitLocker To Go)** aus.



3. Um die erzwungene Verschlüsselung nutzen zu können, muss auch die entsprechende Methode über die Einstellung **Methode für erzwungene Verschlüsselung von Wechseldatenträgern** ausgewählt werden. Auf den anderen Reitern können Sie entsprechende Benachrichtigungen für Endbenutzer eingeben.



4.2 Einstellungen in Richtlinien

Damit DriveLock ein unverschlüsseltes USB-Speichermedium mit BitLocker To Go verschlüsseln kann, müssen Sie als erstes eine Richtlinie mit den entsprechenden BitLocker To Go-Einstellungen konfigurieren.

Legen Sie folgende Einstellungen fest:

1. Allgemeine Einstellungen
2. Einstellungen für die Verwendung verschlüsselter Laufwerke
   - Zertifikats-basierte Laufwerks-Wiederherstellung
   - Administrator-Kennwort für die Verschlüsselung
3. Einstellungen für die Erzwungene Verschlüsselung

In einer Beispielkonfiguration werden alle notwendigen Schritte erläutert.

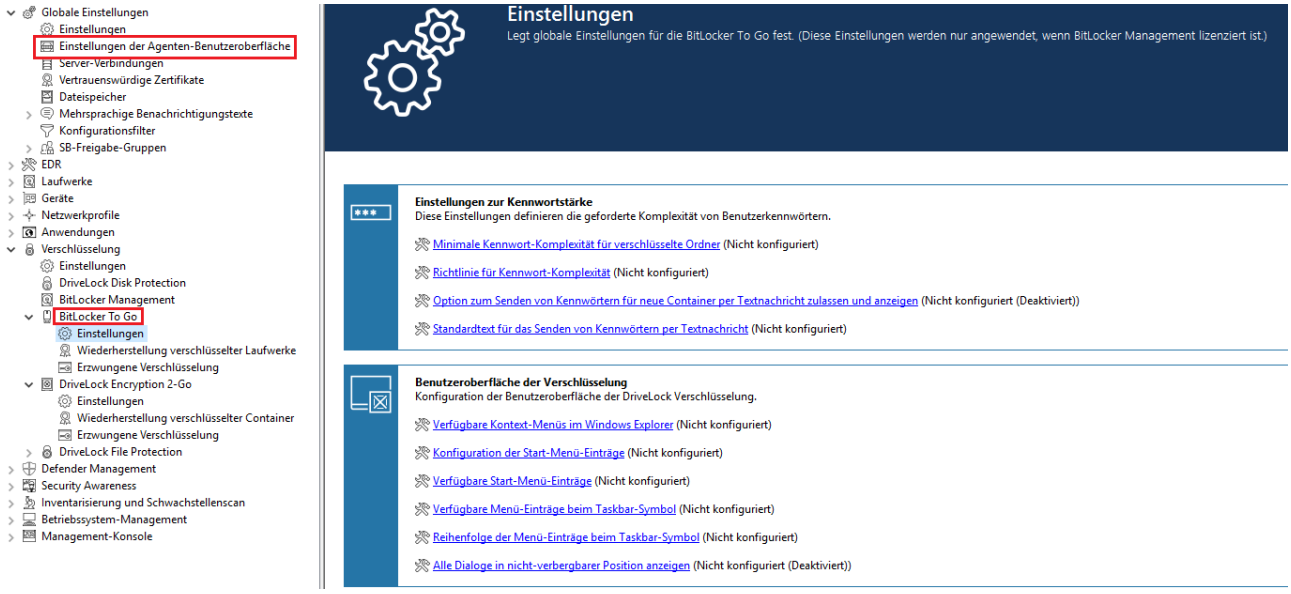
Sobald Sie die Konfiguration abgeschlossen, gespeichert und auf die DriveLock Agenten zugewiesen haben, wird beim Benutzer im Startmenü ein neuer Eintrag **DriveLock BitLocker To Go** angelegt, mit Untermenüs zur Wiederherstellung, Verschlüsselung, Verbindung und Kennwortänderung der jeweiligen USB-Speichermedien.

Bei der nächsten Verbindung eines USB-Speichermediums mit dem DriveLock Agenten wird ein unverschlüsseltes Laufwerk sofort verschlüsselt. DriveLock leitet die Benutzer durch den Verschlüsselungsprozess. Bereits verschlüsselte USB-Speichermedien werden im Unternehmensnetzwerk erkannt, nicht mehr neu verschlüsselt und können verwendet werden.

> Hinweis: Bitte beachten Sie, dass sämtliche Kennwörter (Benutzer oder Administrator) den Komplexitätsregeln entsprechen sollten (8 Zeichen, Großbuchstabe, Kleinbuchstabe, Zahl, Sonderzeichen - z.B. DriveLock1$)

4.2.1 Allgemeine Einstellungen für BitLocker To Go

Sie können folgende Richtlinien-Einstellungen vornehmen, um die Verwendung von BitLocker To Go auf DriveLock Agenten zu konfigurieren:



1. **Einstellungen der Agenten-Benutzeroberfläche** im Knoten **Globale Einstellungen**:
   - Durch Setzen der **Einstellungen für Taskbar-Informationsbereich** können Sie die Art der Benutzerbenachrichtigungen in der Taskleiste konfigurieren. Der Eintrag für BitLocker To Go kann hier an beliebige Stelle verschoben werden.
2. Einstellungen unter **BitLocker To Go**:
   - **Minimale Kennwort-Komplexität für verschlüsselte Ordner**:
     Geben Sie hier einen Wert für die Komplexität der verwendeten Kennwörter an. Wenn Sie als Wert **Kennwort-Richtlinie verwenden** auswählen, müssen Sie genaue Anforderungen definieren.
   - **Richtlinie für Kennwort-Komplexität**:
     Definieren Sie hier die minimalen Anforderungen, die Benutzer bei Eingabe eines BitLocker To Go-Kennworts beachten müssen.
   - Weitere Einstellungen unter **Kennwortstärke** und **Benutzeroberfläche der Verschlüsselung**:
     Die Einstellungen wirken sich auf die Anzeige von BitLocker To Go im Startmenü, in der Taskleiste oder im Windows Explorer aus und sind identisch mit den entsprechenden Einstellungen für Encryption 2-Go.
   - **BitLocker To Go-Medien verwalten, die nicht mit DriveLock verschlüsselt sind**: Aktivieren Sie diese Einstellung, damit Wiederherstellungsinformationen für Wechselmedien, die nicht mit DriveLock verschlüsselt sind, auf den DES hochgeladen werden können. Dazu muss die zertifikatsbasierte Laufwerks-Wiederherstellung sowie die erzwungene Verschlüsselung konfiguriert sein.

Informationen zu den Auswirkungen der Einstellungen finden Sie unter BitLocker To Go auf dem DriveLock Agenten.

4.2.2 Wiederherstellung verschlüsselter Laufwerke

In diesem Abschnitt wählen Sie zunächst das Hauptzertifikat aus (bzw. erstellen eines neu), das für die Wiederherstellung unbedingt benötigt wird und vergeben in einer Administrator-Kennwort-Regel ein Administrator-Kennwort, das für die Verschlüsselung der USB-Speichermedien verwendet wird.

4.2.2.1 Administrator-Kennwort

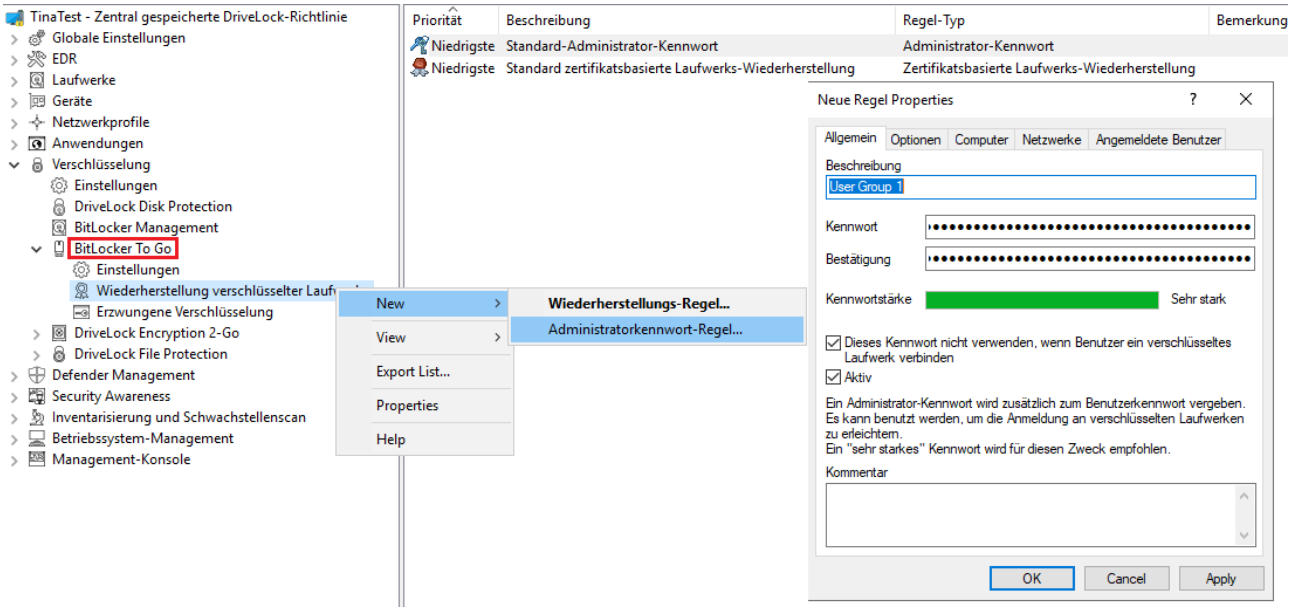
Mithilfe eines zentralen Administrator-Kennworts kann auf verschlüsselte Wechseldatenträger zugegriffen werden.

Hinweis: Achten Sie auf eine ausreichende Komplexität des Administrator-Kennworts.

Sie haben die Möglichkeit, zusätzlich zu diesem zentralen Kennwort weitere Administrator-Kennwort-Regeln anzulegen und diese unterschiedlich zu priorisieren. Die Verwendung unterschiedlicher Kennwörter erhöht die Sicherheit.

Um eine neue Administrator-Regel anzulegen, öffnen Sie das Kontextmenü von **Wiederherstellung verschlüsselter Laufwerke** und wählen dann **Administrator-Kennwort-Regel**.

Sie können dabei die Kennwort-Regeln für bestimmte **Angemeldete Benutzer** oder Benutzergruppen, **Computer** oder **Netzwerke** einschränken. Hierzu geben Sie auf den Reitern im Dialog die entsprechenden Informationen ein. Siehe Anwendungsfälle.



4.2.2.2 Zertifikatsbasierte Laufwerks-Wiederherstellung

Vor Erstellung eines verschlüsselten USB-Speichermediums müssen Sie ein Hauptzertifikat wählen, das aus einem öffentlichen und privaten Schlüsselpaar besteht. Weitere Informationen finden Sie im Kapitel Verschlüsselungzertifikate.

Sie können entweder ein neues Zertifikat erstellen oder ein existierendes verwenden. Weitere Informationen finden Sie im Kapitel Verschlüsselungszertifikate erzeugen.

Sie können auch mehrere Wiederherstellungs-Regeln mit unterschiedlichen Zertifikaten anlegen, die über die Reiter Computer, Benutzer, Netzwerke eingeschränkt und unter-

schiedlich priorisiert werden können. Dies ist dann sinnvoll, wenn unterschiedliche Benutzer eine Wiederherstellung verschlüsselter Daten durchführen dürfen.

Hinweis: Es sollte mindestens das Standard-Wiederherstellungszertifikat (niedrigste Priorität) verwendet werden.

In diesem Dialog sind keine weiteren Angaben nötig.

4.2.3 Erzwungene Verschlüsselung

Die Standard-Verschlüsselungs-Regel ist immer vorhanden. Sie können bei Bedarf weitere Regeln für bestimmte Angemeldete Benutzer, Gruppen, Computer oder Netzwerke anlegen. Siehe Anwendungsfälle.

Bei Bearbeitung der ersten Verschlüsselungs-Regel ist bereits eine Beschreibung auf dem Reiter **Allgemein** eingegeben. Geben Sie einen Kommentar sowie einen eigenen Text hinzu, der im Benutzerauswahldialog angezeigt wird.

Auf dem Reiter **Einstellungen** können Sie die Standard-Einstellungen verwenden oder folgende Optionen auswählen:

- **Administratorkennwort verwenden. Benutzer nicht fragen**: Bei Aktivierung dieser Option wird nur das Administrator-Kennwort verwendet. Benutzer werden bei der Verschlüsselung nicht nach Eingabe eines eigenen Kennworts gefragt.
- **Nutzer nach persönlichem Kennwort fragen**: Bei dieser Einstellung wird der Benutzer nach dem persönlichen Kennwort gefragt.
- **Administratorkennwort versuchen**: Der Benutzer wird zunächst nicht nach dem eigenen Kennwort gefragt. Nur wenn DriveLock das Speichermedium nicht automatisch laden kann, weil z.B. das Administrator-Kennwort nicht übereinstimmt, wird der Benutzer nach dem eigenen Kennwort gefragt.

  Hinweis: Diese Option setzt voraus, dass Sie unter **Wiederherstellung verschlüsselter Laufwerke** ein Administrator-Kennwort gesetzt haben.

- **Verschlüsselungsverfahren**: Wählen Sie eine passende Verschlüsselungsmethode aus. Beachten Sie hierbei folgendes:
  - Als Standardoption ist **AES (256 Bit Schlüssellänge)** ausgewählt.
  - Wählen Sie **AES (128 Bit Schlüssellänge)** aus, wenn Ihnen die Kompatibilität zu älteren System wichtig ist.

- **AES-XTS (128 oder 256 Schlüssellänge)** Verschlüsselungsverfahren können nur ab Windows 10 1511 verwendet werden. Mit XTS AES verschlüsselte Laufwerke sind auf älteren Versionen von Windows nicht zugänglich.

4.3 Beispielkonfiguration für eine Verschlüsselung mit BitLocker To Go

Führen Sie die folgenden Anweisungen in der angegebenen Reihenfolge durch, um Wechseldatenträger (USB-Speichermedien) mit BitLocker To Go zu verschlüsseln bzw. für die Verwendung freizugeben.

Hinweis: Weiterführende Informationen zu den jeweiligen Arbeitsschritten finden Sie unter den Verweisen.

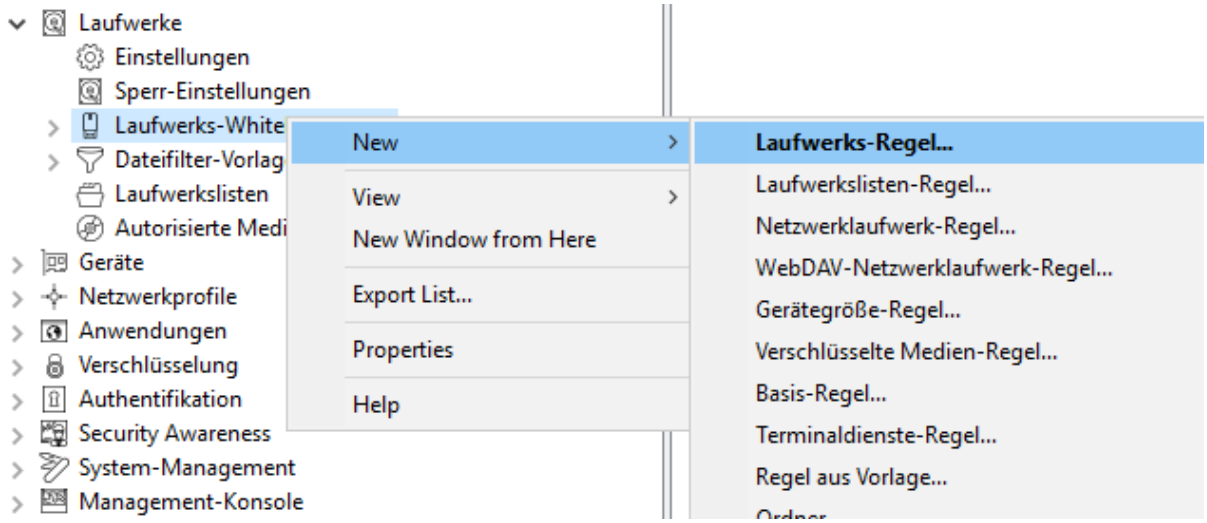
1. Erstellen Sie eine Richtlinie (oder öffnen Sie eine bereits vorhandene), in der Sie die Einstellungen für BitLocker To Go setzen wollen.

   Hinweis: Überprüfen Sie, dass BitLocker Management in dieser Richtlinie lizenziert und die Option unter **Lizenzierte Computer** ausgewählt ist.

2. Öffnen Sie in der Richtlinie den Knoten **Verschlüsselung** und wählen den Unterknoten **Einstellungen** aus. Hier legen Sie zunächst die Verschlüsselungsmethode fest.

   Hinweis: Wenn Sie hier keine Auswahl treffen, ist Encryption 2 Go die Standard-Verschlüsselungsmethode.

3. Wählen Sie die Option **Verfügbare Verschlüsselungsmethoden**.
4. Klicken Sie im Dialog auf **Einstellen auf festen Wert** und setzen Sie ein Häkchen bei **Wechseldatenträger-Verschlüsselung (BitLocker To Go)**. Speichern Sie Ihre Einstellungen und schließen Sie den Dialog.
5. Öffnen Sie den Knoten **Laufwerke**. Bei den **Sperr-Einstellungen** für **USB-angeschlossene Laufwerke** übernehmen Sie die Standardeinstellung **Nicht konfiguriert (Gesperrt)**.
6. Öffnen Sie aus dem Unterknoten **Laufwerks-Whitelist-Regeln** das Kontextmenü, wie in der Abbildung gezeigt. Hier wählen Sie die Option **Laufwerks-Regel** aus.

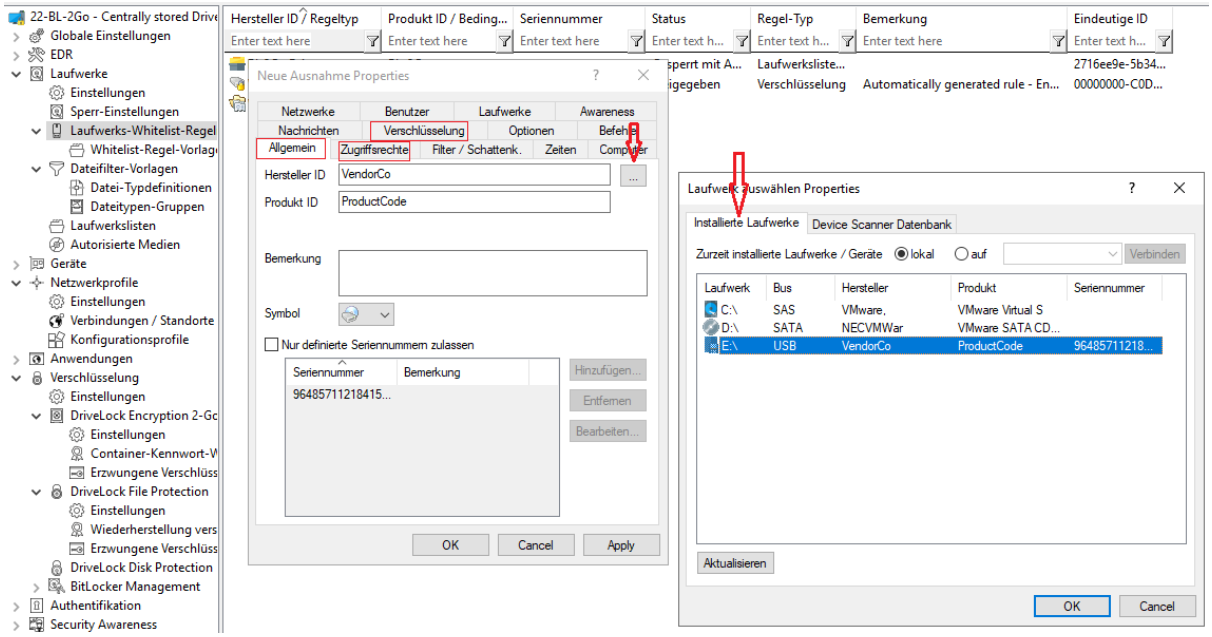


7. Erstellen Sie eine Laufwerks-Regel für das entsprechende USB-Laufwerk. Ein Beispiel finden Sie hier.
8. Als nächstes öffnen Sie wieder den Knoten **Verschlüsselung** und darin den Unterknoten **BitLocker Management**. Hier gehen Sie direkt zu **BitLocker To Go** und wählen zunächst die Option **Wiederherstellung verschlüsselter Laufwerke**
9. Hier sind bereits zwei Standard-Regeln angelegt, die nicht gelöscht werden können.
   - Öffnen Sie als erstes die **Administrator-Kennwort-Regel**. Legen Sie ein komplexes Administrator-Kennwort fest.
   - Als zweites öffnen Sie die Regel für die **Zertifikatsbasierte Laufwerks-Wiederherstellung**. Die Angabe eines Zertifikats ist notwendig, da Sie dieses zur Wiederherstellung benötigen. Entweder erstellen Sie hier ein neues Zertifikat oder wählen ein bereits existierendes aus. Speichern Sie Ihre Einstellungen und schließen Sie den Dialog.
10. Dann öffnen Sie das Kontextmenü der Option **Erzwungene Verschlüsselung**, klicken auf **Neu** und dann **Verschlüsselungs-Regel**.
    Im nachfolgenden Dialog geben Sie auf dem Reiter **Allgemein** eine Beschreibung ein (bei der ersten Regel ist in diesem Textfeld bereits die Beschreibung **Standard-Einstellungen für die erzwungene Verschlüsselung** eingetragen).
    Auf dem Reiter **Einstellungen** übernehmen Sie die Standardeinstellungen: **Nutzer nach persönlichem Kennwort fragen** und dazu die Option **Administratorkennwort versuchen**.
    Durch diese Einstellung wird sichergestellt, dass DriveLock im Hintergrund auf das Administrator-Kennwort zugreifen kann.
11. Als letztes weisen Sie Ihre Richtlinie allen oder bestimmten DriveLock Agenten zu.

4.3.1 Laufwerks-Whitelist-Regel anlegen

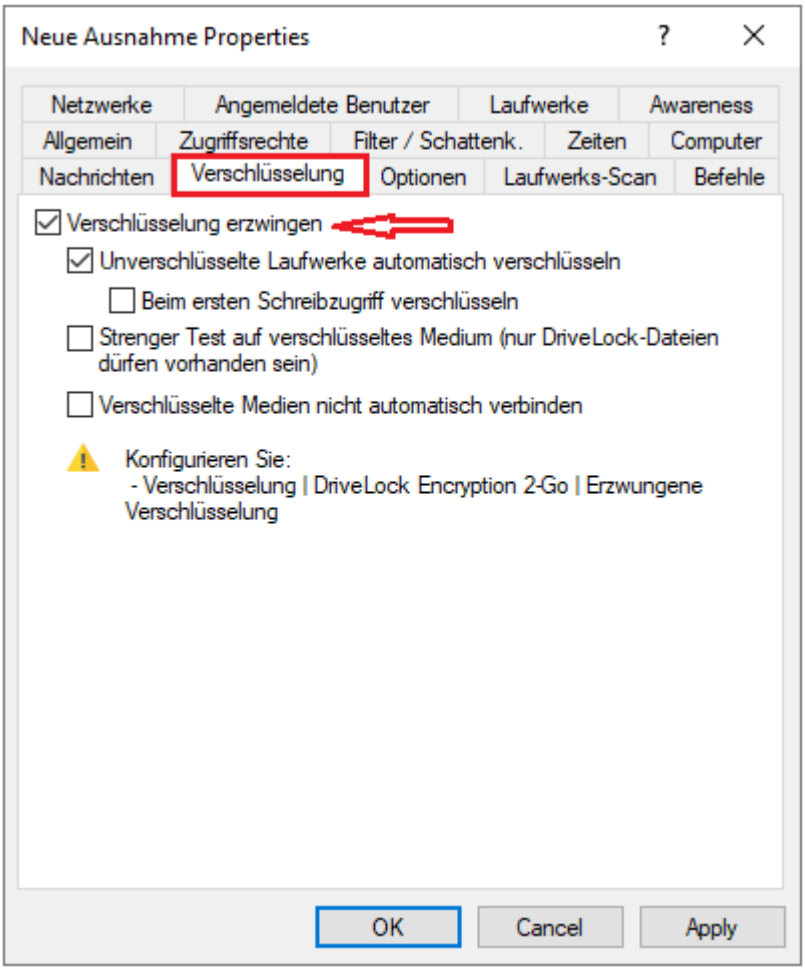
Gehen Sie folgendermaßen vor:

1. Auf dem Reiter **Allgemein** suchen Sie als erstes das USB-Laufwerk aus der Liste der **Installierten Laufwerke** aus.
   Im Beispiel unten ist dies das USB-Laufwerk **E:** mit der Hersteller ID **VendorCo**.



2. Auf dem Reiter **Zugriffsrechte** geben Sie an, dass Sie das Laufwerk erlauben wollen. Mehr zum Thema Whitelist-Regeln erstellen finden Sie im Administrationshandbuch auf DriveLock Online Help.

3. Auf dem Reiter **Verschlüsselung** ist standardmäßig nichts ausgewählt.
   - Hier setzen Sie als erstes ein Häkchen bei **Verschlüsselung erzwingen**. Damit wird sichergestellt, dass das verbundene und erlaubte USB-Laufwerk verschlüsselt sein muss, um verwendet werden zu können.



Hinweis: Diese Option kann dazu führen, dass die Zugriffsrechte angepasst werden, um das gewünschte Verhalten zu ermöglichen.

- Setzen Sie als zweites ein Häkchen bei **Unverschlüsselte Laufwerke automatisch verschlüsseln**, damit die Verschlüsselung beim Einstecken eines unverschlüsselten USB-Laufwerks gestartet wird und sich auf dem DriveLock Agenten ein Assistent öffnet, der den Benutzer durch die Verschlüsselung führt.
- **Beim ersten Schreibzugriff verschlüsseln**: Unverschlüsselte Laufwerke dürfen zwar gelesen werden, aber vor dem Schreiben muss das Laufwerk verschlüsselt werden.

Speichern Sie Ihre Einstellungen und schließen Sie den Dialog.

4.4 BitLocker To Go-Wiederherstellung

Für den Fall, dass ein Benutzer das Kennwort für den Zugriff auf ein verschlüsseltes USB-Speichermedium vergessen hat oder dieses Kennwort aus anderen Gründen nicht mehr ver-

fügbar ist, stellt DriveLock BitLocker To Go einen Wiederherstellungsmechanismus zur Verfügung.

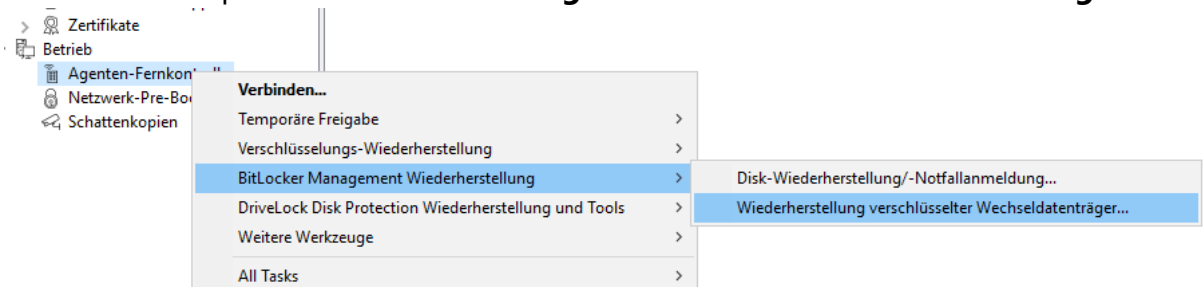
Das Kennwort kann auch dann zurückgesetzt werden, wenn der Client-Computer sich aktuell nicht im Unternehmensnetzwerk befindet.

Das eingesetzte Challenge-Response-Verfahren ähnelt sehr stark dem Verfahren zur temporären Offline-Freigabe für den Zugriff auf gesperrte Laufwerke oder Geräte. DriveLock leitet Benutzer dabei durch den Wiederherstellungsprozess. Der Administrator (oder ein Helpdesk-Mitarbeiter) verwendet die DriveLock Management Konsole, um den angeforderten Antwortcode zu erzeugen.

4.4.1 Wiederherstellungsprozess

Gehen Sie folgendermaßen vor:

1. Öffnen Sie in der DriveLock Management Konsole den Knoten **Betrieb** und hier den Unterknoten **Agenten-Fernkontrolle**.
2. Wählen Sie **BitLocker Management Wiederherstellung** aus dem Kontextmenü aus und dann die Option **Wiederherstellung verschlüsselter Wechseldatenträger...** .



3. Der Benutzer am Client-Computer hat in der Zwischenzeit den Wiederherstellungsassistenten aufgerufen und sich den **Anforderungscode** anzeigen lassen. Lassen Sie sich diesen übermitteln.
4. Geben Sie diesen **Anforderungscode** nun in den Dialog **Offline-Kennwort-Wiederherstellung** ein, Copy & Paste funktioniert hier. Mit dem Anforderungscode wird die auf dem DES gespeicherte Information zu dem verschlüsselten USB-Speichermedium gesucht. In dem Textfeld wird dann angezeigt, wann und von welchem Benutzer das USB-Speichermedium zuletzt verschlüsselt wurde.
5. Im nächsten Dialog wird ein **Antwortcode** generiert, den Sie dem Benutzer mitteilen müssen.

6. Der Benutzer gibt nun seinerseits den **Antwortcode** am Client-Computer ein. Im anschließenden Dialog kann ein neues Benutzerkennwort für das USB-Speichermedium vergeben werden.

4.4.2 Wiederherstellung im DriveLock Operations Center (DOC)

Die Wiederherstellung von verschlüsselten USB-Speichermedien mit Anfrage- und Antwort-Code kann auch über das DriveLock Operations Center (DOC) durchgeführt werden.

Gehen Sie folgendermaßen vor:

1. Öffnen Sie das **DOC**.
2. Wählen Sie im Menü **Sicherheitskontrollen** die Ansicht **Verschlüsselung** aus und hier den Tab **Wiederherstellung**. Wählen Sie den Reiter **BitLocker To Go Wiederherstellung**.
3. Der Benutzer am Client-Computer hat in der Zwischenzeit den Wiederherstellungsassistenten aufgerufen und sich den **Anforderungs- bzw. Wiederherstellungscode** anzeigen lassen.
   Lassen Sie sich diesen übermitteln.
4. Geben Sie dann den **Anforderungs- bzw. Wiederherstellungscode** in Ihre DOC-Maske ein.
5. Wählen Sie die passende **Zertifikatsdatei** aus und geben das dazugehörige Kennwort ein.
6. Klicken Sie auf **Antwortcode generieren** und teilen Sie diesen dem Benutzer mit.
7. Der Benutzer gibt nun seinerseits den **Antwortcode** am Client-Computer ein. Im anschließenden Dialog kann ein neues Benutzerkennwort für das USB-Speichermedium vergeben werden.

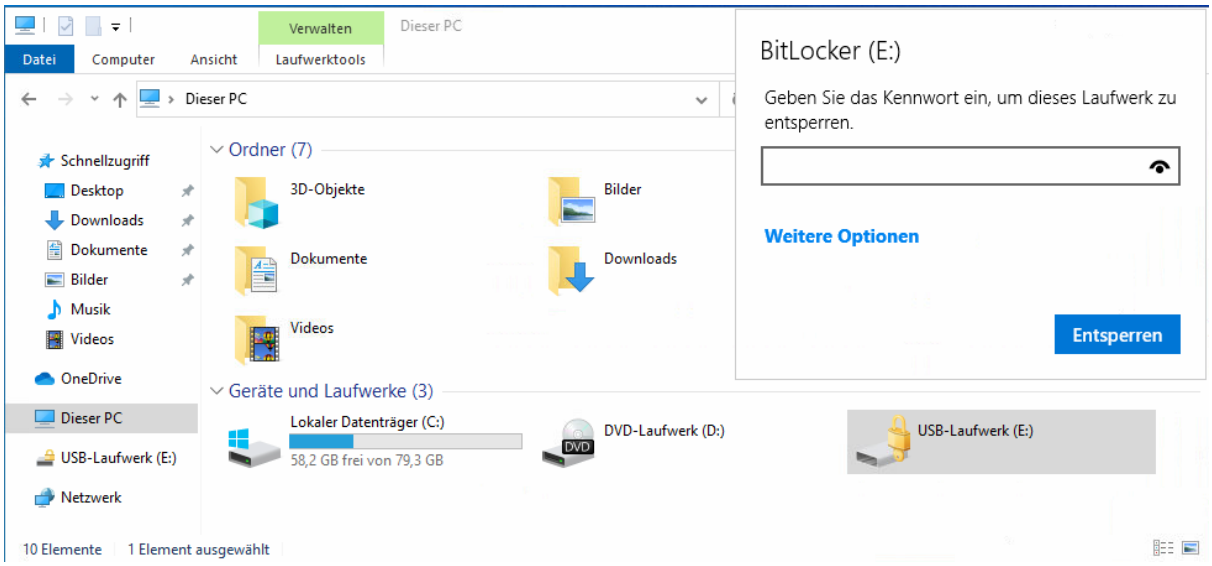
4.5 DriveLock Agent

4.5.1 BitLocker To Go auf dem DriveLock Agenten

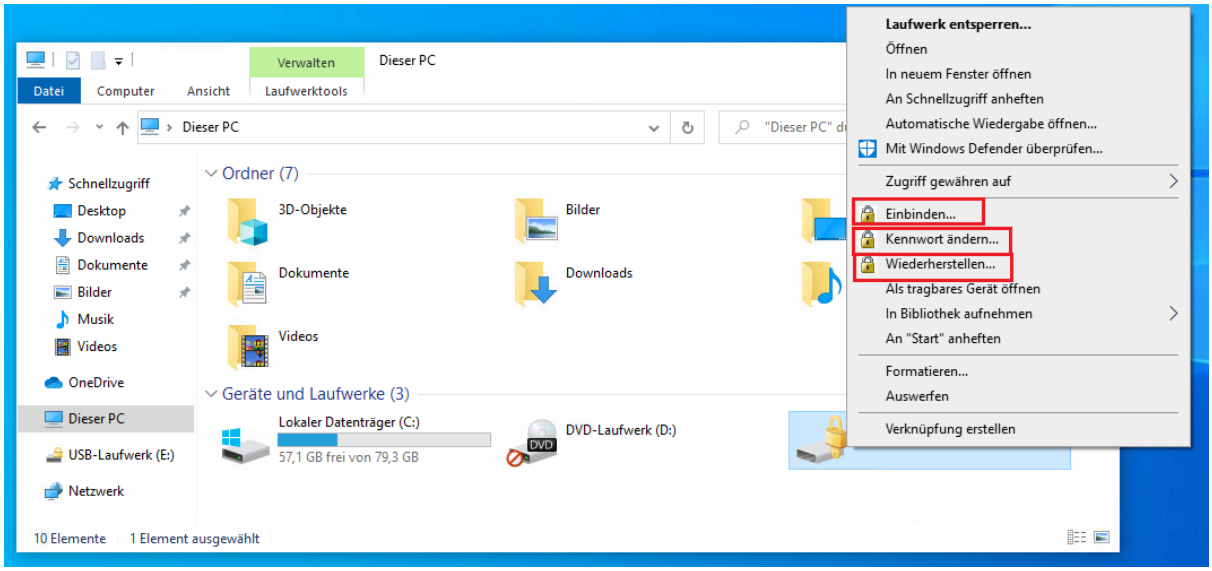
Beim Einstecken eines externen USB-Speichermediums oder externen Laufwerks am DriveLock Agenten können dem Benutzer je nach Richtlinien-Einstellung folgende Optionen angeboten werden:

1. **Entsperren eines verschlüsselten Laufwerks**

   Zum Entsperren eines mit BitLocker To Go verschlüsselten Laufwerks erscheint sofort ein Dialog zur Kennworteingabe. Somit kann zügig entsperrt und auf die vorhandenen Daten zugegriffen werden.



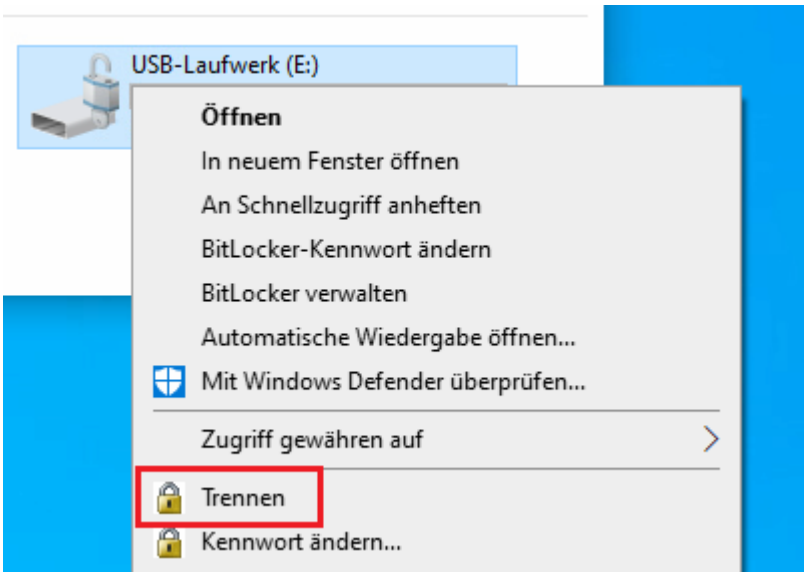
2. **Verschiedene Optionen im Kontextmenü im Windows Explorer:**



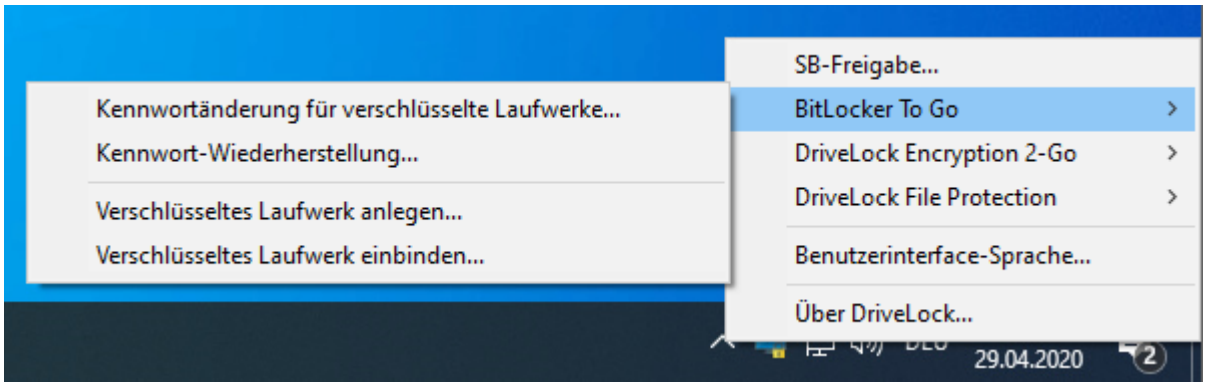
- **Einbinden...**
  Wenn Sie ein mit BitLocker To Go verschlüsseltes Laufwerk einbinden wollen, öffnet sich nach Klick auf diesen Menüeintrag ein Assistent, wo Sie den entsprechenden Laufwerksbuchstaben auswählen und das Kennwort eingeben können. Diese Option kann auch so konfiguriert sein, dass das Kennwort als Administratorkennwort vorgegeben ist und dann automatisch eingetragen wird.
- **Kennwort ändern...**
  Um das Kennwort eines verschlüsselten Laufwerks zu ändern, klicken Sie auf diesen Menüeintrag. Auch hier öffnet sich ein Assistent, wo Sie zunächst Ihr altes und dann Ihr neues Kennwort eingeben können.
- **Wiederherstellen...**

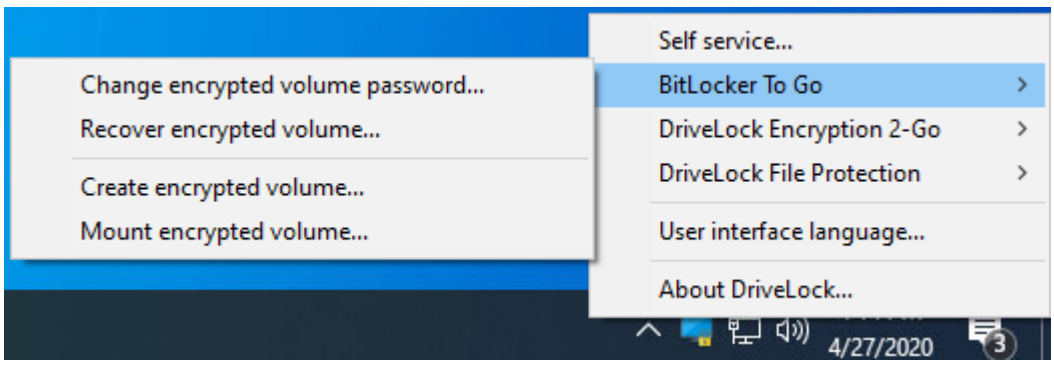
Verwenden Sie diesen Menübefehl, um das Kennwort wiederherzustellen. Der Wiederherstellungsprozess eines verschlüsselten Laufwerks findet zwischen Administrator und Benutzer statt. Weitere Informationen finden Sie hier.

- **Trennen**
  Verwenden Sie diesen Menübefehl um das Laufwerk zu sperren, auch ohne Administratorrechte zu haben.



3. **Sofern eingestellt, können die verschiedenen Optionen für BitLocker To Go auch aus der Taskleiste heraus gewählt werden, siehe Abbildung:**





4.6 Verschiedene Anwendungsfälle

Für folgende DriveLock BitLocker To Go-Optionen sind Anwendungsfälle denkbar:

- Vergabe des Administrator-Kennworts
- Erzwungene Verschlüsselung

4.6.1 Administrator-Kennwort-Regeln

a. **Sie vergeben kein Administrator-Kennwort und erlauben Benutzern, selbst ein Kennwort zu vergeben:**
   - Der Benutzer wählt das Kennwort für die Verschlüsselung bei der Initialverschlüsselung selbst. Das verschlüsselte Laufwerk kann nur automatisch entschlüsselt werden, wenn es dem Benutzer erlaubt ist, das Kennwort zu speichern. An jedem anderen Computer muss es beim Verbinden eingegeben werden.

b. **Sie vergeben ein Administrator-Kennwort und erlauben Benutzern, selbst ein Kennwort zu vergeben:**
   - Der Benutzer vergibt bei der Initialverschlüsselung ein eigenes Kennwort.
   - Das Administrator-Kennwort kann verwendet werden, um die Daten an Unternehmensrechnern mit DriveLock Agent automatisch zu entschlüsseln. Der Benutzer muss somit kein Kennwort eingeben.

c. **Sie vergeben ein Administrator-Kennwort und wählen eine Verschlüsselung mit Administrator-Kennwort:**
   - Der Benutzer kann bei der Initialverschlüsselung kein eigenes Kennwort vergeben
   - Der Wechseldatenträger kann nur an Unternehmensrechnern mit DriveLock Agent entschlüsselt werden
   - Beim Verbinden des verschlüsselten Wechseldatenträgers muss der Benutzer kein Kennwort eingeben
   - Außerhalb des Unternehmens bzw. auf Unternehmensrechnern ohne DriveLock Agent können die Daten nicht entschlüsselt werden

d. **Sie erstellen mehrere Administrator-Kennwort-Regeln und setzen dabei Filter für Benutzer bzw. Computer und wählen eine Verschlüsselung mit Administrator-Kennwort:**
   - Der Benutzer kann bei der Initialverschlüsselung kein eigenes Kennwort vergeben

- Der Wechseldatenträger kann nur an Unternehmensrechnern mit DriveLock Agent entschlüsselt werden
- Beim Verbinden des verschlüsselten Wechseldatenträgers muss der Benutzer kein Kennwort eingeben
- Außerhalb des Unternehmens bzw. auf Unternehmensrechnern ohne DriveLock Agent können die Daten nicht entschlüsselt werden
- Der Zugang wird auf bestimmte Benutzer oder auf gewisse Computer (z.B. in einer Abteilung oder einem Team) beschränkt:
  Sie erstellen eine Administrator-Kennwort-Regel, die auf Benutzergruppe A beschränkt ist. Benutzer A1 verschlüsselt einen USB-Stick (Erzwungene-Verschlüsselung mit Administrator-Kennwort) mit Administrator-Kennwort.
  Folge:
  Der USB-Stick kann nur entschlüsselt werden, wenn ein Benutzer aus Benutzergruppe A an einem Unternehmensrechner angemeldet ist.
  Beispiele:
  - In der Personalabteilung verschlüsselte USB-Sticks können nur von den Benutzern der Personalabteilung entschlüsselt werden
  - In der Forschungsabteilung verschlüsselte USB-Sticks können nur an Computern der Forschungsabteilung entschlüsselt werden

Achtung: Achten Sie auf die Priorität und die auf den Reitern **Angemeldete Benutzer**, **Computer** und **Netzwerk** gesetzten Filtermöglichkeiten.

4.6.2 Verschlüsselungs-Regeln

a. **Sie wählen eine bestimmte Benutzergruppe aus, für die Ihre Regel gelten soll:**
   - Benutzergruppe A kann ein eigenes Kennwort vergeben
   - Benutzergruppe B kann kein eigenes Kennwort vergeben

b. **Sie wählen bestimmte Unternehmensrechner aus, für die Ihre Regel gelten soll:**
   - Für USB-Speichermedien, die an den Computern des Betriebsrates verschlüsselt werden, wird kein Administrator-Kennwort zusätzlich hinzugefügt.
   - USB-Speichermedien, die an den Computern der Entwicklungsabteilung verschlüsselt wurden, können nur innerhalb des Unternehmens entschlüsselt werden.

5 DriveLock Encryption 2-Go

DriveLock Encryption 2-Go bietet eine sichere Verschlüsselung externer Datenträger (wie z.B. USB-Sticks oder SD-Karten) und das sichere Löschen von Dateien mit Hilfe standardisierter, irreversibler Verfahren.

5.1 Allgemeines

DriveLock unterscheidet zwei Arten von Laufwerken:

- Laufwerke basierend auf einer Datei (Container-Datei)
- Laufwerke basierend auf einer existierenden Partition

Die DriveLock Container-Datei ist eine Datei mit der Dateiendung *.dlv. Sie kann auf allen Typen von Speichermedien oder auf einer Netzwerkfreigabe gespeichert werden. Zur Nutzung eines Containers verbindet DriveLock diesen mit einem vordefinierten oder freien Laufwerksbuchstaben, so dass dieser wie jedes andere Laufwerk innerhalb des Windows Explorer verwendet werden kann.

Die DriveLock Partition ist eine normale Partition, die von DriveLock verschlüsselt wird. Es ist möglich, ZIP-Laufwerke, USB- / FireWire-Festplatten und USB-Speichersticks sowie andere Massenspeichergeräte zu verschlüsseln.

> Hinweis: Bei bestimmten Hardware-Speichermedien ist das Erstellen einer verschlüsselten Partition nicht möglich. Bitte kontaktieren Sie hierzu den Hersteller des Speichermediums. Das Laufwerk, das die Windows Betriebssystemdateien enthält (typischerweise C:\), kann nicht über diesen Weg verschlüsselt werden. Es muss die DriveLock Disk Protection verwendet werden, wenn es nötig ist, auch die System Partition zu verschlüsseln.

5.1.1 Verschlüsselungsverfahren

Verschlüsselte Laufwerke werden als einzelne Container-Dateien realisiert. Der Zugriff auf diese Dateien ist kennwortgeschützt. Zusätzlich gibt es bei DriveLock die Möglichkeit, das Kennwort mit Hilfe eines Offline-Verfahrens zurückzusetzen.

Verschlüsselte Daten scheinen aus zufälligen Buchstaben und Zahlen zu bestehen. Innerhalb eines verschlüsselten Laufwerks sind auch Datei- und Verzeichnisnamen ebenso wie freier Platz verschlüsselt. Die Verschlüsselungsmethode definiert, auf welche Art und Weise Daten auf dem jeweiligen Laufwerk verschlüsselt werden.

Auf aktuellen Systemen erfolgt die Ver- und Entschlüsselung durch **Verschlüsselungsverfahren**, die in der Open SSL implementiert sind:

- AES (Advanced Encryption Standard) wird empfohlen
- Zur Auswahl stehen in den DriveLock Dialogen noch zusätzliche Verschlüsselungsalgorithmen: Triple DES, Blowfish, Twofish, CAST 5 und Serpent.

Mit einem Hash Algorithmus verschlüsselt DriveLock das Kennwort, mit welchem das verschlüsselte Laufwerk ver- bzw. entschlüsselt wird. DriveLock unterstützt folgende **Hash-Verfahren**:

- SHA-256 und SHA -512 (beide auch als FIPS-Variante) werden empfohlen
- Zur Auswahl stehen in den DriveLock Dialogen noch zusätzliche Hash-Verfahren: RIPEMD-160 und WHIRLPOOL

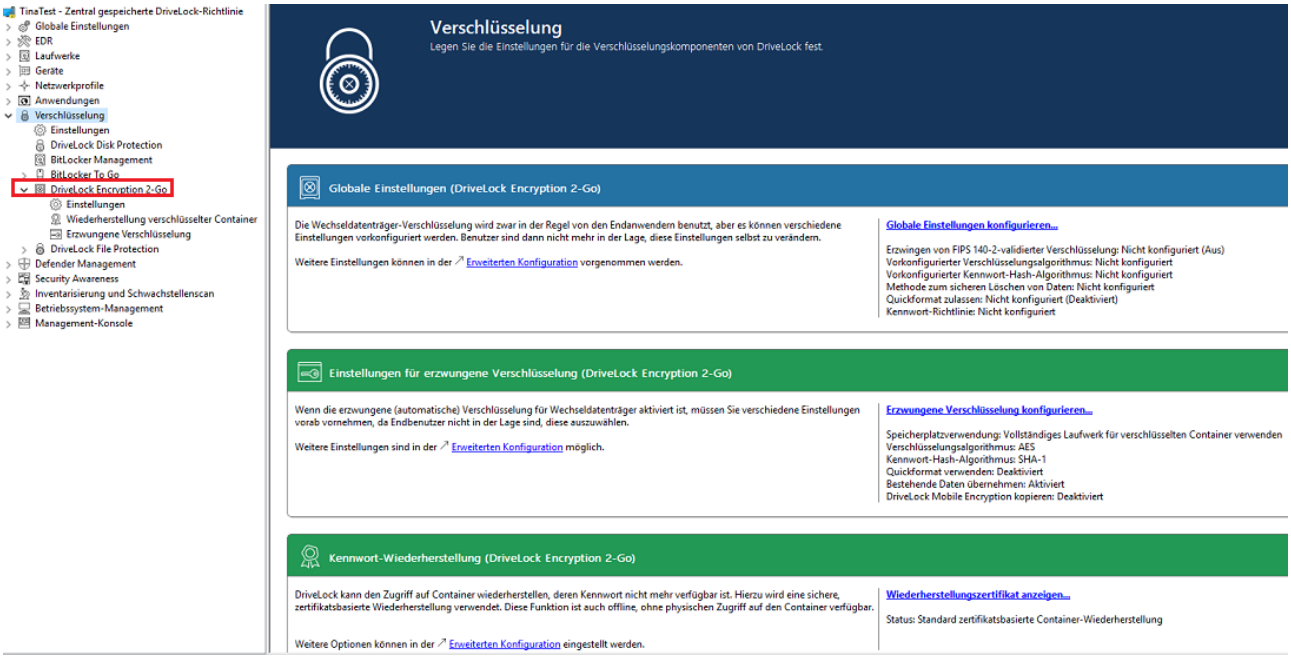
5.2 Einstellungen in Richtlinien

5.2.1 Einstellungen

In der Taskpad-Ansicht können Sie in folgenden Abschnitten Einstellungen für Encryption 2-Go vornehmen:

- Globale Einstellungen für die Verschlüsselung von Wechseldatenträgern
- Einstellungen für erzwungene Verschlüsselung
- Konfiguration der Kennwort-Wiederherstellung für verschlüsselte Medien

Wenn Sie auf **Erweiterte Konfiguration** klicken, werden Ihnen alle vorhandenen Einstellungen angezeigt.



5.2.1.1 Globale Einstellungen konfigurieren

Die globalen Einstellungen für Encryption 2-Go umfassen folgende Konfigurationsmöglichkeiten:

- **Verschlüsselungsverfahren für verschlüsselte Laufwerke**
  Hier wählen Sie aus, welches Verschlüsselungsverfahren angewendet werden soll
- **Kennwort-Hashverfahren für verschlüsselte Laufwerke**
  Hier wählen Sie das Hashverfahren für die verschlüsselten Laufwerke aus
- **Methode zum sicheren Löschen von Daten**
  Sie können festlegen, welche Methode verwendet wird, damit Daten auf sichere Weise gelöscht werden.
- **Erzwingen von FIPS 140-2-validierter Verschlüsselung**
  Wenn Ihr Unternehmen es erfordert, FIPS 140-2 zertifizierte Algorithmen zu verwenden, können Sie dies hier konfigurieren. Wenn Sie den FIPS-Modus aktivieren, wählen Sie eine der folgenden beiden Optionen:
  - **Aus**: Wählen Sie diese Einstellungen, um auch auf Container bzw. verschlüsselte Laufwerke zuzugreifen, die nicht mit FIPS 140-2 zertifizierten Verfahren verschlüsselte wurden. Wenn ein Benutzer einen neuen verschlüsselten Container erstellt, wird jedoch ein FIPS 140-2 zertifiziertes Verfahren verwendet.
  - **Ein (Nicht-FIPS-Verschlüsselung ausschalten)**: Verwenden Sie diese Option, wenn Sie sicherstellen müssen, dass ausschließlich FIPS 140-2 zertifizierte Verfahren sowohl für die Ver- als auch für die Entschlüsselung angewendet werden können. Jeder mit Nicht- FIPS 140-2 zertifizierten Verfahren verschlüsselte Container bzw. Laufwerk kann jetzt nicht mehr entschlüsselt werden.
- **Quick-Format für verschlüsselte Container zulassen**
  Um den Zeitraum zum Erstellen eines verschlüsselten Containers zu verkürzen, wählen Sie die Option **Quick-Format für verschlüsselte Container erlauben**. Dadurch wird nicht der komplette Container durch den DriveLock Agenten verschlüsselt, sondern nur die benötigten Teile.
- **Minimale Kennwort-Komplexität für verschlüsselte Laufwerke**
- **Richtlinie für Kennwort-Komplexität**
  Eine Kennwort-Komplexitäts-Richtlinie enthält alle Anforderungen, die ein Benutzerkennwort erfüllen muss, wenn es erstellt wird. Diese enthält die Mindestanzahl an Zeichen und die Anzahl der Sonderzeichen, die ein Kennwort enthalten muss.

5.2.1.2 Einstellungen für erzwungene Verschlüsselung

Die Einstellungen für die erzwungene Verschlüsselung umfassen folgende Konfigurationsmöglichkeiten:

Wählen Sie zunächst das zu verwendende Verschlüsselungsverfahren aus und konfigurieren Sie einen Hash-Algorithmus.

- Quick-Format verwenden
- **Bestehende Daten erhalten**: Wählen Sie diese Option, wenn DriveLock alle unverschlüsselten Dateien er-halten und mit verschlüsseln soll. Dazu wird ein temporäres Verzeichnis (Standardmäßig im Benutzerprofil von Windows) erstellt, der verschlüsselte Container dort erzeugt, die vorhandenen Daten vom Laufwerk dort hinein kopiert und zum Schluss der Container komplett auf den Wechseldatenträger verschoben.
- **DriveLock Mobile Encryption auf unverschlüsselten Teil kopieren**: Sie haben außerdem die Möglichkeit, festzulegen, ob die Mobile Encryption Anwendung auf Wechseldatenträger während der automatischen Verschlüsselung kopiert werden soll. Dies ermöglicht die Nutzung auch auf Rechnern, auf denen DriveLock nicht installiert ist.
- **Vollständiges Laufwerk für verschlüsselten Container verwenden**: Aus technischer Sicht muss DriveLock die voraussichtliche maximale Größe des verschlüsselten Containers berechnen, wenn die Daten erhalten bleiben sollen. Das kann dazu führen, dass etwas Speicherplatz nicht von dem verschlüsselten Laufwerk verwendet wird. Wenn Sie erreichen möchten, dass der Container den kompletten verfügbaren Speicherplatz verwenden kann, aktivieren Sie diese Funktionalität. In Verbindung mit dieser Option wird DriveLock den kompletten restlichen verfügbaren Speicherplatz (sofern verfügbar) auffüllen. Dazu erstellt DriveLock versteckte Systemdateien in entsprechender Größe. Wenn es mehr als 2GB freien Platz gibt, werden mehrere Dateien erstellt, jede maximal 2GB groß.
- **Unverschlüsselten Bereich auf Laufwerk freilassen**: Wählen Sie diese Option, wenn Sie nicht den vollständigen Platz auf einem Laufwerk für die Verschlüsselung verwenden möchten. Geben Sie eine Größe an und legen Sie fest, ob die Zahl als absoluter Wert oder als Prozentwert verstanden werden soll.

5.2.1.3 Einstellungen für die Kennwort-Wiederherstellung

Dieser Abschnitt beschreibt die beiden notwendigen Konfigurationsschritte, um später bei Bedarf das Kennwort bei einem verschlüsselten Container (zum Beispiel bei einem zwangsverschlüsselten USB-Stick) zurücksetzen zu können. Damit Sie die Funktionalität der Offline-Kennwort-Wiederherstellung nutzen zu können, müssen Sie vor der Erstellung des ersten verschlüsselten Containers ein Hauptzertifikat bestehend aus einem öffentlichen und privaten Schlüsselpaares erzeugen.

Klicken Sie dazu auf **Neues Wiederherstellungszertifikat erzeugen**. Dadurch wird der Assistent für die Erzeugung des Hauptzertifikates gestartet.

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

Sie können das Zertifikat und das Kennwort zusätzlich auf dem Server abspeichern damit sie vom DOC verwendet werden können, ohne dass die Datei lokal vorhanden sein muss.

Folgen Sie dann den Anweisungen hier ab Schritt 3.

5.2.1.4 Erweiterte Einstellungen

Im Folgenden finden Sie einen Überblick über alle verfügbaren Einstellungen für Encryption 2-Go.

Einstellung	Funktionalität
Einstellungen zur Verschlüsselungsstärke	
Erzwingen von FIPS 140-2-validierter Verschlüsselung	Aktivieren Sie mit dieser Einstellung den FIPS-Modus.
Verschlüsselungsverfahren für verschlüsselte Laufwerke	Konfigurieren Sie den zu verwendenden Verschlüsselungsalgorithmus.
Kennwort-Hashverfahren für verschlüsselte Laufwerke	Geben Sie hier das Hash-Verfahren an.
Quick-Format für verschlüsselte	Definieren Sie hie, ob Sie das Quick-Format

Einstellung	Funktionalität
Container zulassen	zulassen wollen.
Einstellungen zur Kennwortstärke	
Minimale Kennwort-Komplexität für verschlüsselte Laufwerke	Die minimal erforderliche Kennwortkomplexität für verschlüsselte Laufwerke sollte so definiert werden, dass sie den Firmenrichtlinien entspricht. Die Komplexität wird auf Basis der verwendeten Zeichen sowie der Kennwortlänge berechnet.
Richtlinie für Kennwort-Komplexität	Eine Kennwortkomplexitäts-Richtlinie enthält alle Anforderungen, die ein Benutzerkennwort erfüllen muss, wenn es erstellt wird. Diese enthält die Mindestanzahl an Zeichen und die Anzahl der Sonderzeichen, die ein Kennwort enthalten muss. DriveLock kann ein Benutzerkennwort auch verweigern, wenn es in einem Wörterbuch vorkommt.
Aussperrungs-Richtlinie für Container	Die Aussperrungs-Richtlinie hilft Brute-Force Angriffe zu unterbinden, indem ein Container nach einer definierten Anzahl von Versuchen ein Passwort einzugeben für eine angegebene Anzahl von Minuten oder für immer gesperrt wird.
Optionen zum Speichern von Kennwörtern verschlüsselter Container	Das gespeicherte Kennwort wird beim Mounten von diesem Container automatisch verwendet. Das hilft bei langen und komplizierten Passwörtern.

Einstellung	Funktionalität
Erzeugung (und Anzeige) von Zufallskennwörtern für neue Container erlauben	Eine zusätzliche Option wird im Erstellungsassistenten angezeigt, mit der Benutzer Zufallskennwörter generieren lassen können.
Optionen zum Senden von Kennwörtern für neue Container per Textnachricht zulassen und anzeigen	Zeigt bei Aktivierung eine zusätzliche Assistentenseite beim Erstellen von Containern an und ermöglicht das Versenden von Kennwörtern per Textnachricht (SMS). Das dazu benötigte SMS-Gateway wird in den Globalen Einstellungen unter **Einstellung Konfigurationseinstellungen für Textnachrichten (SMS)** konfiguriert. Weitere Informationen in der Dokumentation DriveLock Administration auf DriveLock Online Help.
Standardtext für das Senden von Kennwörtern per Textnachricht	Legt den Standardtext für das Senden von Kennwörtern per Textnachricht fest.
Einstellungen zur Kennwort-Wiederherstellung	
Wiederherstellungsmethoden für verschlüsselte Container	DriveLock stellt für die Wiederherstellung verlorengegangener Kennwörter bei verschlüsselten Containern zwei Methoden zur Verfügung: • Offline-Wiederherstellung über ein Challenge-Response-Verfahren: Mit Unterstützung eines Assistenten kann das Kennwort eines verschlüsselten Containers zurückgesetzt werden, auch wenn der Computer derzeit nicht mit dem Firmennetzwerk verbunden ist.

Einstellung	Funktionalität
	• Online-Wiederherstellung über lokal installierte Zertifikate: Ist diese Option aktiviert, kann ein Kennwort auch ohne ein Challenge-Response-Verfahren zurückgesetzt werden, vorausgesetzt das dafür notwendige Zertifikat mit privatem und öffentlichem Schlüsselpaar ist lokal auf dem entsprechenden Rechner verfügbar.
Endbenutzer-Kontaktinformation für Offline-Kennwort-Wiederherstellung	Wenn ein Benutzer sein persönliches Kennwort für den Zugriff auf den Container bzw. das verschlüsselte Laufwerk vergessen hat, kann er über das Symbol in der Taskleiste oder das Startmenü den Assistenten zur Kennwort-Wiederherstellung aufrufen. Dort wird ihm am Anfang ein Text angezeigt, der über diesen Menüpunkt frei vorgegeben werden kann.
Benutzeroberfläche der Verschlüsselung	
Verfügbare Kontext-Menüs im Windows Explorer	Diese Einstellungen legen alle über das Kontextmenü verfügbaren Optionen fest. Die Einstellung „Nicht konfiguriert“ aktiviert alle Optionen
Konfiguration der Start-Menü-Einträge	Sie können definieren, ob die DriveLock Startmenüeinträge angezeigt und wie diese angeordnet werden sollen.
Verfügbare Start-Menü-Einträge	Diese Option definiert die Startmenüeinträge, die angezeigt werden sollen

Einstellung	Funktionalität
Verfügbare Menü-Einträge beim Taskbar-Symbol	Sie können definieren, ob alle Menüpunkte bei Nutzung des Taskleisten-Symbols angezeigt werden sollen
Reihenfolge der Menü-Einträge beim Taskbar-Symbol	Sie können definieren, in welcher Reihenfolge die Menüpunkte bei Nutzung des Taskleisten-Symbols angezeigt werden sollen.
Alle Dialoge in nicht-verbergbarer Position anzeigen	Geben Sie an, ob Dialoge verborgen werden können.
Einstellungen für verschlüsselte Laufwerke	
Dateisystem für verschlüsselte Laufwerke	Das Dateisystem für neue verschlüsselte Laufwerke kann FAT, exFAT oder NTFS sein.
Clustergröße für verschlüsselte Laufwerke	Stellen Sie hier die Clustergröße für verschlüsselte Laufwerke ein.
Verfügbare Laufwerksbuchstaben für verschlüsselte Laufwerke	Konfigurieren Sie hier die Laufwerksbuchstaben, die automatisch an verschlüsselte Laufwerke vergeben werden
Erzwungener Laufwerksbuchstabe für ein verschlüsseltes Laufwerk	Durch Aktivieren dieser Einstellung kann nur ein verschlüsseltes Laufwerk mit dem definierten Buchstaben verbunden werden
Größenbeschränkung für verschlüsselte Laufwerke	Geben Sie einen Wert an, der die maximale Größe von verschlüsselten Containern angibt.

Einstellung	Funktionalität
Benutzer-Einschränkungen	
Keine Historie für verbundene Laufwerke erstellen	Diese Option verhindert die Verlaufserstellung verbundener Datenträger
Erstellung von DriveLock Mobile Encryption nicht zulassen	Die Mobile Encryption Anwendung (MEA) wird zur Entschlüsselung von Daten auf einem Rechner benötigt, der keinen DriveLock Agenten installiert hat. DriveLock kann die MEA zusammen mit einer Autostart-Datei auf ein Laufwerk kopieren, wenn darauf eine verschlüsselte Container-Datei abgelegt wird. Deaktivieren Sie diese Option, wenn dies für den Benutzer nicht möglich sein soll.
Nur mit dieser DriveLock-Lizenz verschlüsselte Container zulassen	Wenn Sie diese Option aktivieren, kann DriveLock nur noch Container öffnen, die von einem Agenten mit der gleichen Lizenz wie der gerade konfigurierten verschlüsselt wurden
Container können nicht mit DriveLock Mobile Encryption geöffnet werden	Die Mobile Encryption Anwendung dient dazu, verschlüsselte Laufwerke oder Container auch auf Systemen zu entschlüsseln, auf denen kein DriveLock installiert ist.
DriveLock Mobile Encryption nicht automatisch auf neuere Version aktualisieren	Normalerweise überprüft DriveLock beim Verbindungsversuch, ob die auf einem Wechseldatenträger vorhandene MEA der aktuellen Version entspricht und ersetzt sie ggf. automatisch mit der aktuellsten Version

5.2.2 Wiederherstellung verschlüsselter Container

Für den Fall, dass ein Benutzer das Kennwort für den Zugriff auf eine verschlüsselte Container-Datei vergessen hat oder dieses Kennwort aus anderen Gründen nicht mehr verfügbar ist, stellt DriveLock Encryption 2-Go zwei Wiederherstellungsmechanismen zur Verfügung.

1. Die Offline-Wiederherstellung verschlüsselter Container funktioniert analog zur Wiederherstellung von Laufwerken bei BitLocker To Go.
    - Das Kennwort kann auch dann zurückgesetzt werden, wenn der Client-Computer sich aktuell nicht im Unternehmensnetzwerk befindet.
    - Das eingesetzte Challenge-Response-Verfahren ähnelt sehr stark dem Verfahren zur temporären Offline-Freigabe für den Zugriff auf gesperrte Laufwerke oder Geräte. DriveLock leitet Benutzer dabei durch den Wiederherstellungsprozess. Der Administrator (oder ein Helpdesk-Mitarbeiter) verwendet die DriveLock Management Konsole, um den angeforderten Antwortcode zu erzeugen.
2. Beim Online-Wiederherstellungsprozess wird auf dem DriveLock Agenten das Verschlüsselungszertifikat benötigt, ein Challenge-Response-Verfahren ist dann nicht nötig.

5.2.2.1 Administrator-Kennwort

Mithilfe eines zentralen Administrator-Kennworts kann auf verschlüsselte Container-Dateien zugegriffen werden.

> Hinweis: Achten Sie auf eine ausreichende Komplexität des Administrator-Kennworts.

Sie haben die Möglichkeit, zusätzlich zu diesem zentralen Kennwort weitere Administrator-Kennwort-Regeln anzulegen und diese unterschiedlich zu priorisieren. Die Verwendung unterschiedlicher Kennwörter erhöht die Sicherheit.

Um eine neue Administrator-Regel anzulegen, öffnen Sie das Kontextmenü von **Wiederherstellung verschlüsselter Laufwerke** und wählen dann **Administrator-Kennwort-Regel**.

Sie können dabei die Kennwort-Regeln für bestimmte **Angemeldete Benutzer** oder Benutzergruppen, **Computer** oder **Netzwerke** einschränken. Hierzu geben Sie auf den Reitern im Dialog die entsprechenden Informationen ein. Siehe die Anwendungsfälle für BitLocker To Go, die analog auch für Encryption 2-Go gelten.

Die Option **Dieses Kennwort nicht verwenden, wenn Benutzer ein verschlüsseltes Laufwerk verbinden** sollte nur dann aktiviert werden, wenn diese Regel innerhalb einer Benutzerauswahl-Regel verwendet wird.

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

- **Mit jeder Art von Verschlüsselung** – Diese Kennung wird immer verwendet.
- **Mit manueller Verschlüsselung** (...) – Diese Kennung wird nur verwendet, wenn die Verschlüsselung durch einen Benutzer über Kommandozeile oder durch das Benutzerinterface von DriveLock erfolgt.
- **Mit erzwungener / automatischer Verschlüsselung** – Diese Kennung wird nur verwendet, wenn die Ver-schlüsselung automatisch durch DriveLock erfolgt (sog. erzwungene Verschlüsselung)

5.2.2.2 Zertifikatsbasierte Container-Wiederherstellung

Vor Erstellung eines verschlüsselten USB-Speichermediums müssen Sie ein Hauptzertifikat wählen, das aus einem öffentlichen und privaten Schlüsselpaar besteht.

Sie können entweder ein neues Zertifikat erstellen oder ein existierendes verwenden. Weitere Informationen finden Sie im Kapitel Einstellungen für die Kennwort-Wiederherstellung.

Sie können auch mehrere Wiederherstellungs-Regeln mit unterschiedlichen Zertifikaten anlegen, die über die Reiter Computer, Angemeldete Benutzer, Netzwerke eingeschränkt und unterschiedlich priorisiert werden können. Dies ist dann sinnvoll, wenn unterschiedliche Benutzer eine Wiederherstellung verschlüsselter Daten durchführen dürfen.

> Hinweis: Es sollte mindestens das Standard-Wiederherstellungszertifikat (niedrigste Priorität) verwendet werden.

In diesem Dialog sind keine weiteren Angaben nötig.

5.2.3 Erzwungene Verschlüsselung

Bevor USB-Datenträger automatisch verschlüsselt werden können (erzwungene Verschlüsselung), müssen Grundeinstellungen getroffen werden. Diese beinhalten u.a. den Verschlüsselungsalgorithmus und andere Rahmenbedingen, wie z.B. die Übernahme bestehender Daten von einem unverschlüsseltem Stick bei der Verschlüsselung oder die Größe des verschlüsselten Bereiches. Hierzu können verschiedene Regeln für bestimmte Benutzer oder Computer angelegt werden, oder beispielsweise Regeln, die nur bei bestimmten Netzwerkverbindungen angewendet werden.

Falls gewünscht, können auch bis zu drei verschiedene dieser Regeln zu einer Benutzerauswahl zusammengefasst werden. Diese wird dem Benutzer angezeigt (z.B. beim Einstecken eines USB-Sticks) und dieser wählt aus den angebotenen Optionen die für ihn passende Verwendungsoption aus.

Beispiele:

- Alle USB-Sticks sollen mit AES verschlüsselt werden.
- Nur die USB-Sticks des Vorstandes sollen mit AES (FIPS-mode) verschlüsselt werden.
- Der Benutzer soll selbst entscheiden können, ob er den Stick komplett oder nur 50% der verfügbaren Kapazität für die Verschlüsselung nutzt.
- Der Benutzer kann zwischen den zwei Optionen auswählen, z.B. 'USB-Laufwerk komplett verschlüsseln' und 'Laufwerk unverschlüsselt nach Bestätigung eines Sicherheitshinweises lesend nutzen'.

5.2.3.1 Verschlüsselungs-Regel

Die Standard-Verschlüsselungs-Regel ist immer vorhanden. Sie können bei Bedarf weitere Regeln für bestimmte Angemeldete Benutzer, Gruppen, Computer oder Netzwerke anlegen. Siehe Anwendungsfälle.

Zur Erstellung wählen Sie im Unterknoten **Erzwungene Verschlüsselung** die Option **Neu** und dann **Verschlüsselungs-Regel**.

Bei Bearbeitung der ersten Verschlüsselungs-Regel ist bereits eine Beschreibung auf dem Reiter **Allgemein** eingegeben. Bei einer neuen Regel geben Sie hier eine Beschreibung ein.

- Geben Sie einen Kommentar sowie einen eigenen Text hinzu, der im Benutzerauswahldialog angezeigt wird. Sie können an dieser Stelle auch eine vorher konfigurierte mehrsprachige Benachrichtigung auswählen.
- Die Option **Diese Regel nicht automatisch anwenden** sollte nur dann aktiviert werden, wenn diese Regel innerhalb einer Benutzerauswahl-Regel verwendet wird.

Auf dem Reiter **Einstellungen** können Sie die Standard-Einstellungen verwenden oder folgende Optionen auswählen:

- **Administratorkennwort verwenden. Benutzer nicht fragen**: Bei Aktivierung dieser Option wird nur das Administrator-Kennwort verwendet. Benutzer werden bei der Verschlüsselung nicht nach Eingabe eines eigenen Kennworts gefragt.

- **Nutzer nach persönlichem Kennwort fragen**: Bei dieser Einstellung wird der Benutzer nach dem persönlichen Kennwort gefragt.
- **Administratorkennwort versuchen**: Der Benutzer wird zunächst nicht nach dem eigenen Kennwort gefragt. Nur wenn DriveLock das Speichermedium nicht automatisch laden kann, weil z.B. das Administrator-Kennwort nicht übereinstimmt, wird der Benutzer nach dem eigenen Kennwort gefragt.

> Hinweis: Diese Option setzt voraus, dass Sie unter **Wiederherstellung verschlüsselter Laufwerke** ein Administrator-Kennwort gesetzt haben.

- **Beim Anlegen Administratorkennwort immer deaktivieren**: Sobald ein Benutzer ein persönliches Kennwort festgelegt hat, wird beim Verschlüsseln des USB-Speichermediums das Administratorkennwort gelöscht. Dadurch kann auf die verschlüsselten Daten nur noch durch Eingabe des Benutzerkennwortes zugegriffen werden.
- **Benutzer können Administratorkennwort beim Anlegen deaktivieren**: Wählen Sie diese Option, wenn es Benutzern ermöglicht werden soll, „private“ USB-Speichermedien ohne Verwendung des Administrator-Kennworts zu erzeugen.
- **Verschlüsselungsverfahren**: Wählen Sie eine passende Verschlüsselungsmethode aus.
- **Vollständiges Laufwerk für verschlüsselten Container verwenden**: DriveLock verwendet den kompletten verfügbaren Speicherplatz für die Verschlüsselung. Aus technischer Sicht muss DriveLock die voraussichtliche maximale Größe des verschlüsselten Containers berechnen, wenn die Daten erhalten bleiben sollen. Das kann dazu führen, dass etwas Speicherplatz nicht von dem verschlüsselten Laufwerk verwendet wird.
- **Aus technischen Gründen freibleibenden Platz auffüllen**: Wenn Sie erreichen möchten, dass der Container den kompletten verfügbaren Speicherplatz verwenden kann, aktivieren Sie diese Funktionalität. In Verbindung mit dieser Option können Sie DriveLock veranlassen, den kompletten restlichen verfügbaren Speicherplatz (sofern verfügbar) aufzufüllen. Dazu erstellt DriveLock eine versteckte Systemdatei in entsprechender Größe.
- **Freien Platz übriglassen x KB** : In manchen Windows 7 Umgebungen, müssen wenige KB frei bleiben, damit überhaupt auf das Laufwerk zugegriffen werden kann.
- **Unverschlüsselten Bereich auf Laufwerk freilassen**: Wählen Sie diese Option, wenn Sie nicht den vollständigen Platz auf einem Laufwerk für die Verschlüsselung

verwenden möchten. Geben Sie eine Größe an und legen Sie fest, ob die Zahl als absoluter Wert oder als Prozentwert verstanden werden soll.

- **Maximale Größe verschlüsselter Container x MB**: Hier können Sie definieren wie groß der verschlüsselte Container maximal sein darf.

Auf dem Reiter **Verschlüsselung** geben Sie das Verschlüsselungs- und Hashverfahren, Dateisystem und Clustergröße an.

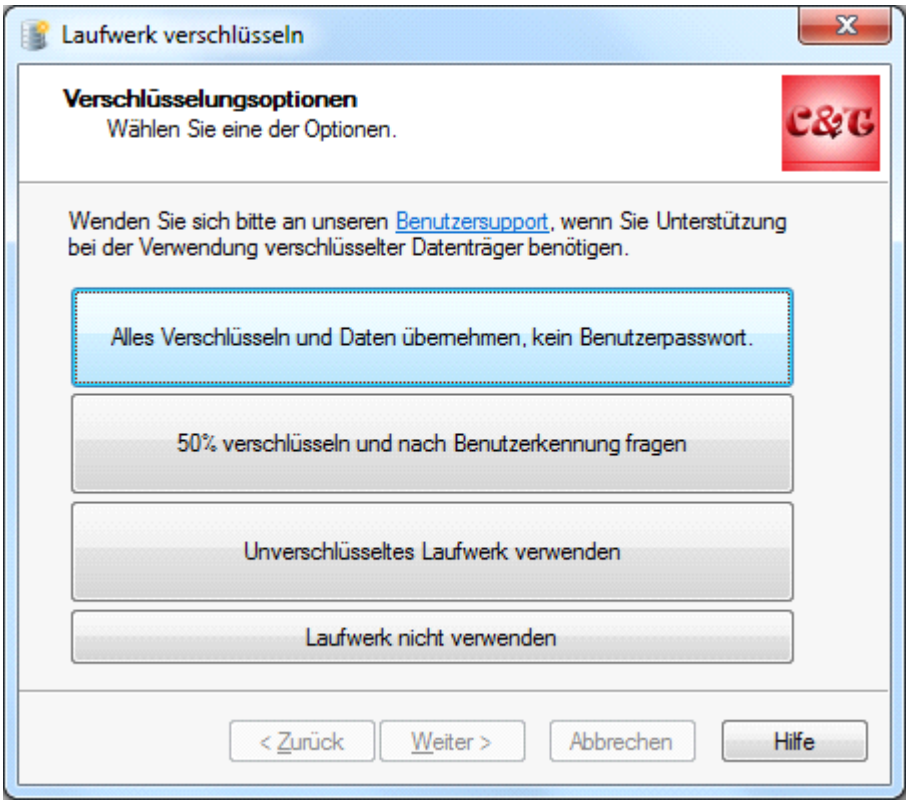
Auf dem Reiter **Dateisystem** können Sie folgende Angaben machen:

- **Bestehende Daten erhalten**: Wählen Sie diese Option, wenn DriveLock alle unverschlüsselten Dateien er-halten und mit verschlüsseln soll. Dazu wird ein temporäres Verzeichnis (Standardmäßig im Benutzerprofil von Windows) erstellt, der verschlüsselte Container dort erzeugt, die vorhandenen Daten vom Laufwerk dort hinein kopiert und zum Schluss der Container komplett auf den Wechseldatenträger verschoben. Sie können auch festlegen, dass dieses temporäre Verzeichnis an einem von Ihnen festgelegtem Platz erstellt wird (Option „Speziellen temporären Ordner während dem Anlegen verwenden").
- **DriveLock Mobile Encryption auf unverschlüsselten Teil kopieren**: Sie haben außerdem die Möglichkeit, festzulegen, ob die Mobile Encryption Anwendung auf Wechseldatenträger während der automatischen Verschlüsselung kopiert werden soll. Dies ermöglicht die Nutzung auch auf Rechnern, auf denen DriveLock nicht installiert ist. Zusätzlich kann eine Autorun.inf Datei mit angelegt werden, worin auch benutzerspezifische Inhalte konfiguriert werden können.
- **Speziellen temporären Ordner während dem Anlegen verwenden**: Sollen vorhandene Daten auf dem Stick übernommen werden, so können Sie hier ein Verzeichnis angeben, in dem das Verzeichnis mit dem temporären Container angelegt werden soll.
- **Verschlüsselte Containerdatei verstecken**: Wenn diese Option aktiviert ist, wird die Datei EEDATA.DLV als „Versteckt" markiert.
- **Dateisysteme, die nicht mehr als 4 GB unterstützen, automatisch auf exFAT oder NTFS umformatieren**

5.2.3.2 Benutzerauswahl-Regel

Eine Benutzerauswahl legt fest, welche Verschlüsselungs- bzw. Verwendungsoptionen ein Benutzerauswahldialog enthält, wenn er dem Benutzer nach dem Verbinden eines Laufwerkes angezeigt wird.

Beispiel, wie ein Benutzerauswahldialog aussehen könnte:



Zur Erstellung wählen Sie im Unterknoten **Erzwungene Verschlüsselung** die Option **Neu** und dann **Benutzerauswahl-Regel**.

Auf dem Reiter **Allgemein** geben Sie eine Beschreibung und ggf. einen Kommentar ein.

Auf dem Reiter **Nachrichten** definieren Sie die Texte, die dann im Benutzerauswahldialog erscheinen werden. Hier werden die Elemente Titel, Untertitel und Hilfetext konfiguriert. Alle Texte können entweder direkt eingegeben oder als zuvor definierte mehrsprachige Benutzernachricht ausgewählt werden.

Auf dem Reiter **Auswählbare Regeln** können Sie über die Schaltfläche **Hinzufügen** bis zu drei vorher angelegten Verschlüsselungs-Regeln konfigurieren. Die Reihenfolge, in der Sie die Regeln hinzufügen, bestimmt auch die Reihenfolge, wie sie im Benutzerauswahldialog angezeigt werden.

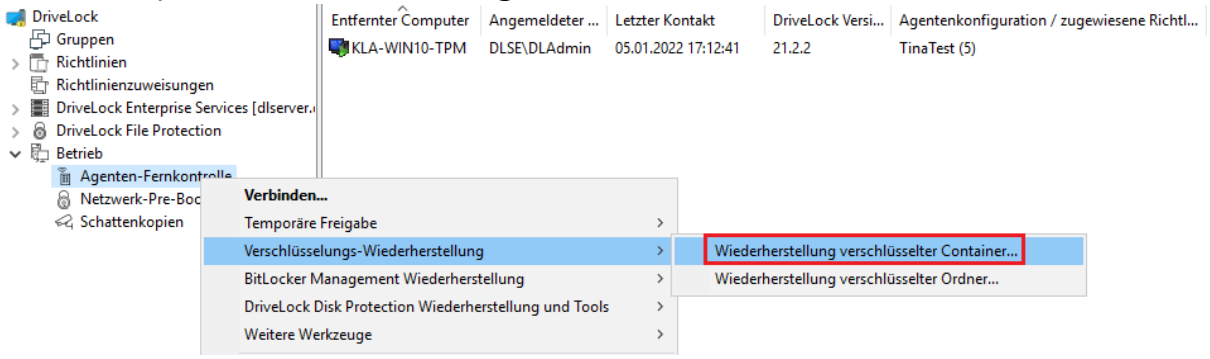
- Wenn Sie die Option **"Unverschlüsselter Zugriff auf Laufwerk" als Auswahl hinzufügen** aktivieren und der Benutzer wählt diese Auswahloption aus, erhält der angemeldete Benutzer Lese- und Schreibzugriff auf das Laufwerk, auch wenn in der Laufwerksregel selbst der Zugriff als generell überhaupt nicht oder als nur lesender Zugriff konfiguriert wurde. Aktivieren Sie die Option „Verwendungsrichtlinie anzeigen, bevor Zugriff erlaubt wird“, um nach Auswahl dieser Alternative durch den Benutzer

vor der Freischaltung noch eine Verwendungsrichtlinie anzuzeigen.

- Im Gegensatz dazu stellt die letzte Option **"Kein Zugriff auf Laufwerk" als Auswahl hinzufügen"** die „Abbrechen"-Schaltfläche dar. Wählt der Benutzer diese Auswahloption, wird das Laufwerk entsprechend den Zugriffsberechtigungen, die in der Laufwerks-Whitelist-Regel konfiguriert wurden, verbunden. Die gleichen Berechtigungen werden auch verwendet, wenn der Benutzer einen der Verschlüsselungs-Assistenten vorzeitig beendet.

5.3 Offline-Wiederherstellungsprozess

1. Öffnen Sie in der DriveLock Management Konsole den Knoten **Betrieb** und hier den Unterknoten **Agenten-Fernkontrolle**.
2. Wählen Sie **Verschlüsselungs-Wiederherstellung** aus dem Kontextmenü aus und dann die Option **Wiederherstellung verschlüsselter Container...** :



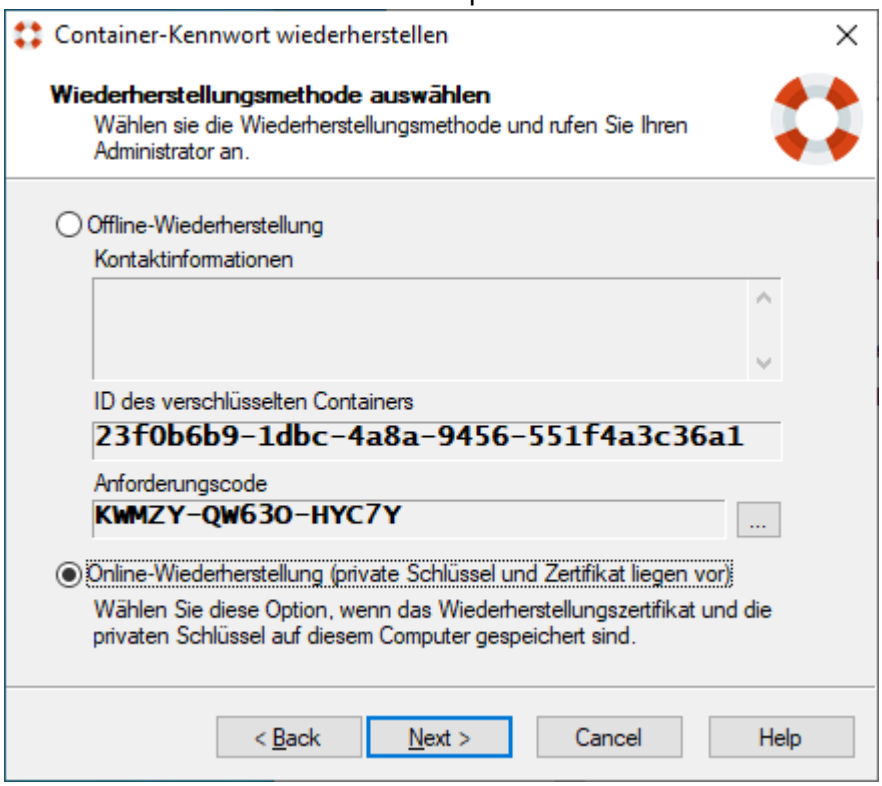
3. Der Benutzer am Client-Computer hat in der Zwischenzeit den Wiederherstellungsassistenten aufgerufen und sich den **Anforderungscode** anzeigen lassen. Lassen Sie sich diesen übermitteln.
4. Geben Sie diesen **Anforderungscode** nun in den Dialog **Offline-Kennwort-Wiederherstellung** ein, Copy & Paste funktioniert hier. Mit dem Anforderungscode wird die auf dem DES gespeicherte Information zu dem verschlüsselten USB-Speichermedium gesucht. In dem Textfeld wird dann angezeigt, wann und von welchem Benutzer das USB-Speichermedium zuletzt verschlüsselt wurde.
5. Im nächsten Dialog wird ein **Antwortcode** generiert, den Sie dem Benutzer mitteilen müssen.
6. Der Benutzer gibt nun seinerseits den **Antwortcode** am Client-Computer ein. Im anschließenden Dialog kann ein neues Benutzerkennwort für das USB-Speichermedium vergeben werden.

5.4 Online-Wiederherstellungsprozess

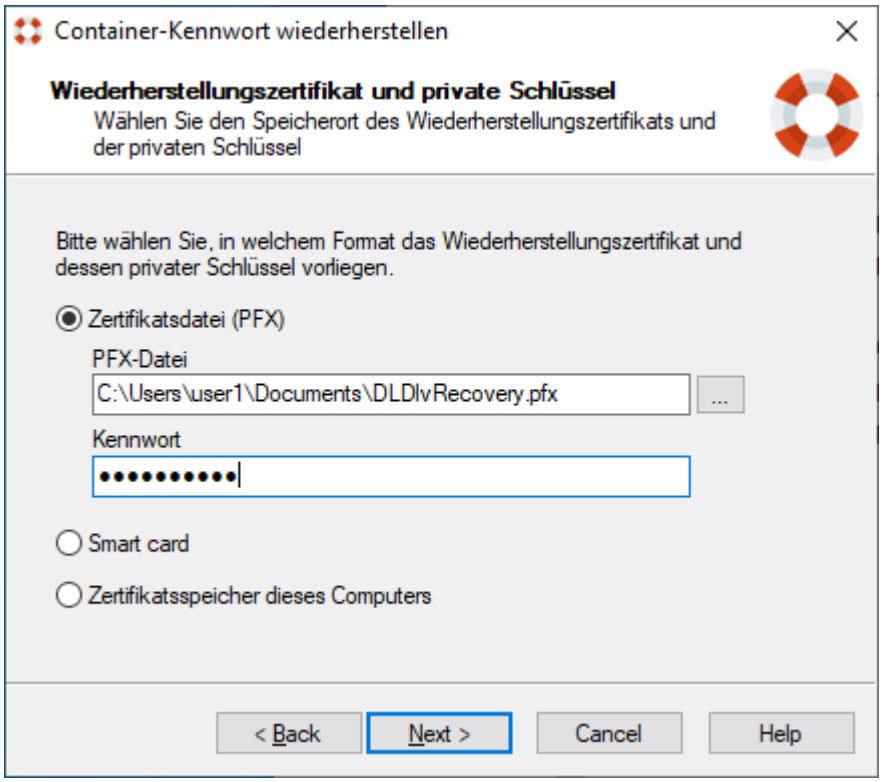
Hinweis: Die Online-Wiederherstellung kann nur dann durchgeführt werden, wenn auf dem DriveLock Agenten ein entsprechendes lokales Zertifikat vorhanden und dieser mit dem Firmennetzwerk verbunden ist.

Der Endbenutzer auf dem DriveLock Agenten führt folgende Schritte im Kennwort-Wiederherstellungsassistenten durch:

1. Wiederherstellungsmethode auswählen
   Der Endbenutzer wählt hier die Option **Online-Wiederherstellung (...)** aus.

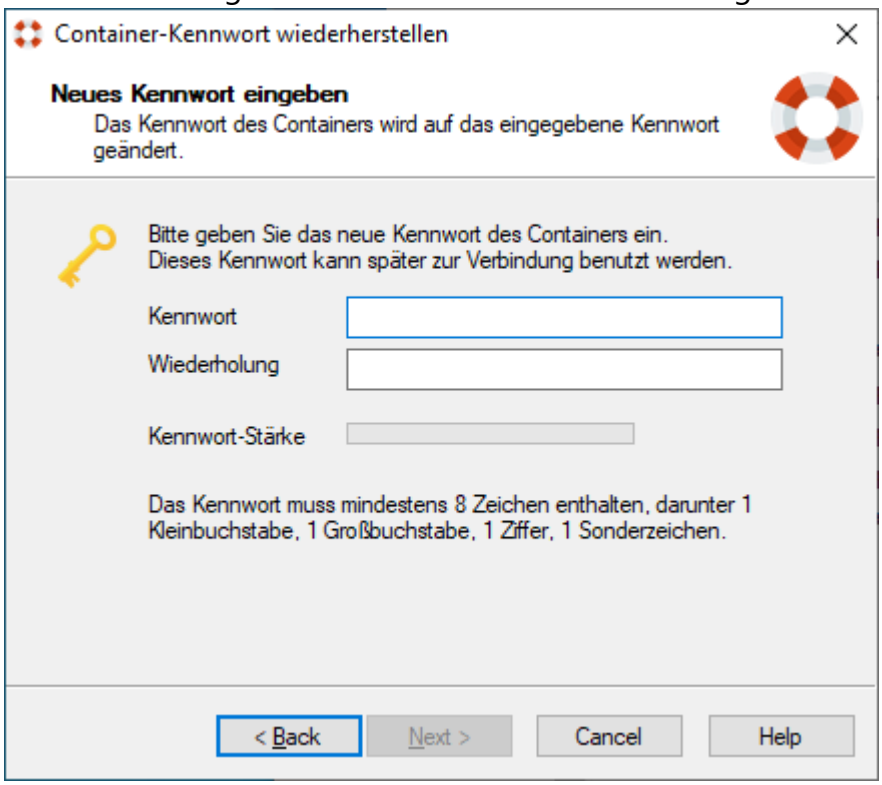


2. Wiederherstellungszertifikat angeben
   Entweder wird der Pfad zur Zertifikatsdatei zusammen mit dem korrekten Kennwort angegeben oder auf eine Smartcard oder auf das Zertifikat im Zertifikatsspeicher verwiesen.



3. Neues Kennwort eingeben

   Im letzten Dialog kann dann ein neues Kennwort vergeben werden.



5.5 Wiederherstellung im DriveLock Operations Center (DOC)

Die Wiederherstellung von verschlüsselten Containern mit Anfrage- und Antwort-Code kann auch über das DriveLock Operations Center (DOC) durchgeführt werden.

Gehen Sie folgendermaßen vor:

1. Öffnen Sie das **DOC**.
2. Wählen Sie den Bereich **Betrieb** aus und hier aus dem Untermenü **Wiederherstellung**, den Reiter **Encryption 2-Go Wiederherstellung**.
3. Der Benutzer am Client-Computer hat in der Zwischenzeit den Wiederherstellungsassistenten aufgerufen und sich den **Anforderungs- bzw. Wiederherstellungscode** anzeigen lassen.
   Lassen Sie sich diesen übermitteln.
4. Geben Sie dann den **Anforderungs- bzw. Wiederherstellungscode** in Ihre DOC-Maske ein.
5. Wählen Sie die passende **Zertifikatsdatei** aus und geben das dazugehörige Kennwort ein.
6. Klicken Sie auf **Antwortcode generieren** und teilen Sie diesen dem Benutzer mit.
7. Der Benutzer gibt nun seinerseits den **Antwortcode** am Client-Computer ein. Im anschließenden Dialog kann ein neues Benutzerkennwort für das USB-Speichermedium vergeben werden.

6 DriveLock File Protection

DriveLock File Protection ermöglicht Ihnen die von privilegierten Nutzern unabhängige bzw. nicht beeinflussbare Verschlüsselung von Dateien und Verzeichnissen. Sie beinhaltet:

- Dateiverschlüsselung auf lokalen Rechnern, zentralen Verzeichnissen eines Servers, externen USB-Datenträgern oder bei Cloud-basierten Diensten (z.B. Dropbox, Microsoft OneDrive, Google Drive)
- AES-NI Unterstützung (hardware-unterstützte, schnelle Verschlüsselung)
- Authentifizierung beim Zugriff auf verschlüsselte Verzeichnisse mit Benutzername/Kennwort oder über X.509-basierte Zertifikate
- Integrierte, voll funktionsfähige Public Key Infrastructure

Hinweis: Für den Einsatz von File Protection wird eine Lizenz benötigt.

Ab Version 2022.2 führt DriveLock ein neues Verschlüsselungsformat ein, das ab dieser Version standardmäßig auf neue DriveLock Agenten angewendet wird. Bei Bestandsagenten wird das alte Format beibehalten. In der DMC gibt es jetzt eine spezielle Richtlinieneinstellung, mit der Sie bei Bedarf verschiedene Verschlüsselungsformate festlegen können.

Achtung: Neues und altes Verschlüsselungsformat sind nicht kompatibel und müssen in separaten Richtlinien abgebildet werden.

6.1 Wie funktioniert DriveLock File Protection?

Zunächst wird ein Verzeichnis "verschlüsselt", d.h. es wird als Verzeichnis markiert, in dem Dateien ausschließlich verschlüsselt abgelegt werden. Dann wird festgelegt, für welchen Benutzer DriveLock File Protection im Hintergrund automatisch und vom Benutzer unbemerkt die Dateien beim Speichern verschlüsselt und beim Öffnen entschlüsselt.

Auf allen Computern, auf denen DriveLock File Protection aktiv ist, wird bei jedem Zugriff auf ein Verzeichnis geprüft, ob es sich um ein markiertes (verschlüsseltes) Verzeichnis handelt. Erkennt DriveLock ein derartiges Verzeichnis, prüft es die Berechtigungen des aktuellen Benutzers und führt ggf. automatisch eine Ver- bzw. Entschlüsselung durch.

Besondere Prozesse, wie zum Beispiel die Durchführung eines Backups oder die Synchronisation von Verzeichnissen können von der automatischen Ver- bzw. Entschlüsselung

ausgenommen werden. Damit wird eine Beeinträchtigung bestehender Systemroutinen vermieden.

Für die Authentifizierung der Benutzer können zwei verschiedene Alternativen verwendet werden:

- Kennwort: Für den Zugriff auf ein verschlüsseltes Verzeichnis muss ein Kennwort eingeben werden
- Zertifikat: Die Authentifizierung erfolgt über ein im Windows Zertifikatsspeicher oder auf einer Smartcard / einem Token hinterlegtes Benutzerzertifikat

Die für eine Verwaltung von Zertifikaten üblicherweise verwendete Public Key Infrastruktur (PKI) ist für DriveLock File Protection nicht notwendig, da DriveLock bereits alle Funktionen dafür mitbringt.

Hinweis: Wenn Sie bereits über eine Active Directory PKI und Benutzerzertifikate verfügen, können Sie diese für die Authentifizierung von Benutzern für DriveLock File Protection verwenden.

Ver- und Entschlüsselungsvorgänge erfolgen im Hintergrund, ohne dass ein Benutzer davon etwas mitbekommt. Dieser Vorgang erfolgt durch bereits im Prozessor vorhandene Verschlüsselungsalgorithmen (AES NI).

Die Verwaltung verschlüsselter Verzeichnisse auf zentralen Laufwerken (z.B. Shares, NAS) erfolgt zentral über die DriveLock Management Konsole (DMC) durch den Administrator. Die Vergabe von Berechtigungen für die Entschlüsselung kann durch eine oder mehrere Personen der Fachabteilung (z.B. die Personalverwaltung) getrennt erfolgen. Dadurch wird zum einen der Administrator von diesen zusätzlichen Aufgaben entlastet, zum anderen kann diesem Administrator auch der Zugriff entzogen werden, so dass auch er nicht in der Lage ist Dateien in diesen Verzeichnissen zu entschlüsseln.

Neben diesen sogenannten zentral verwalteten Verzeichnissen können die Benutzer auch eigene Verzeichnisse bestimmen (bzw. anlegen) und dort Dateien sicher verschlüsselt speichern (z.B. als privates lokales Verzeichnis, auf einem USB-Stick oder als Verzeichnis bei Dropbox oder einem anderen Cloud-Dienstleister). Auch hier können zusätzliche Benutzer autorisiert werden, die diese Dateien dann entschlüsseln bzw. Dateien verschlüsselt dort ablegen können.

Hinweis: Weitere Informationen über Erstellung und Verwendung von privaten Verzeichnissen finden Sie im DriveLock User Guide auf DriveLock Online Help..

6.1.1 Unterstützte Verschlüsselungsverfahren

DriveLock File Protection unterstützt als Verschlüsselungsverfahren:

- AES: Der Advanced Encryption Standard (AES) ist ein symmetrisches Kryptoverfahren, welches als Nachfolger für DES bzw. 3DES im Oktober 2000 vom National Institute of Standards and Technology (NIST) als Standard bekannt gegeben wurde. Nach seinen Entwicklern Joan Daemen und Vincent Rijmen wird er auch Rijndael-Algorithmus genannt. DriveLock verwendet AES-256, welches nach aktuellem Stand der Technik als ausreichend sicher für die Verschlüsselung vertraulicher Informationen angesehen wird.

Mit einem Hash Algorithmus verschlüsselt DriveLock das Kennwort, mit welchem das verschlüsselte Laufwerk ver- bzw. entschlüsselt wird. DriveLock unterstützt folgende Hash-Verfahren:

- SHA: Das NIST (National Institute of Standards and Technology) entwickelte zusammen mit der NSA (National Security Agency) eine zum Signieren gedachte sichere Hash-Funktion als Bestandteil des Digital Signatur Algorithms (DSA) für den Digital Signature Standard (DSS). Die Funktion wurde 1994 veröffentlicht. Diese als Secure Hash Standard (SHS) bezeichnete Norm spezifiziert den sicheren Hash-Algorithmus (SHA) mit einem Hash-Wert von 160 Bit Länge für Nachrichten mit einer Größe von bis zu 264 Bit. Der Algorithmus ähnelt im Aufbau dem von Ronald L. Rivest entwickelten MD4. Der sichere Hash-Algorithmus existiert zunächst in zwei Varianten, SHA-0 und SHA-1, die sich in der Anzahl der durchlaufenen Runden bei der Generierung des Hashwertes unterscheiden. Das NIST hat im August 2002 drei weitere Varianten („SHA-2“) des Algorithmus veröffentlicht, die größere Hash-Werte erzeugen. Es handelt sich dabei um den SHA-256, SHA-384 und SHA-512 wobei die angefügte Zahl jeweils die Länge des Hash-Werts (in Bit) angibt.

6.2 File Protection konfigurieren

Bevor Sie DriveLock File Protection verwenden können, sind einige Entscheidungen zu treffen und die daraus resultierenden Konfigurationsschritte durchzuführen.

Folgende Fragen sind dabei zu beantworten:

- Wie verwalte ich die Benutzerzertifikate für die Authentifizierung?
- Welche Einstellungen gelten für die Ver- bzw. Entschlüsselung?

- Welche Funktionen stehen dem Benutzer auf seinem Computer zur Verfügung?
- Wie soll die Verzeichnisstruktur aussehen, in dem die Daten bzw. Dateien verschlüsselt abgelegt werden?

Für die Verwaltung von Benutzerzertifikaten stehen Ihnen insbesondere die folgenden Möglichkeiten offen:

- Die Verwaltung erfolgt durch den Benutzer - ein persönliches (selbst signiertes) Zertifikat kann vom Benutzer in der DriveLock Anwendung erstellt werden.
- Die Verwaltung erfolgt durch DriveLock, die Benutzerzertifikate (öffentlicher Schlüssel) werden in der Datenbank von DriveLock gespeichert
- Benutzerzertifikate werden in einer vorhandenen PKI im Microsoft Active Directory außerhalb von DriveLock verwaltet
- Die Zertifikate der Benutzer werden in einer mit Microsoft Windows kompatiblen Umgebung außerhalb von DriveLock verwaltet.

Die verschiedenen Optionen für die Ver- und Entschlüsselung und die Konfiguration der Benutzeroptionen finden Sie unter Richtlinienkonfiguration für Clients.

Das Kapitel Verschlüsselte Laufwerke zentral verwalten beschreibt das Anlegen und Verwalten von zentral verwalteten Verzeichnissen.

6.2.1 Master-Zertifikat für die Schlüsselverwaltung einrichten

Bevor Sie mit Hilfe des DriveLock Enterprise Service eigene Zertifikate verwalten können, müssen Sie, ggf. pro Mandant, ein Master-Zertifikat erstellen bzw. einrichten, mit Hilfe dessen alle weiteren Benutzer-Zertifikate signiert und ausgestellt werden können.

In den Servereigenschaften legen Sie fest, ob Sie das Master-Zertifikat des Mandanten root für alle Mandanten verwenden oder für jeden Mandanten eine eigenes Master-Zertifikat erstellen wollen.

- Öffnen Sie hierzu DriveLock Enterprise Services / Server / Doppel-Klick <Servername> / Optionen und markieren Sie **Mandantenfähiges Zertifikatsmanagement aktivieren**.

So erstellen Sie ein Master-Zertifikat für die DriveLock File Protection:

1. Öffnen Sie DriveLock Enterprise Services / Mandanten
   Rechts-Klick <Mandantenname> / Alle Aufgaben / **MasterZertifikat konfigurieren**.
   Sollte die Zertifikatsverwaltung noch nicht eingerichtet worden sein, erscheint ein

Einrichtungsassistent. Klicken Sie Weiter.

2. Wenn Sie ein bereits vorhandenes eigenes Zertifikat verwenden, wählen Sie die Option **Bestehendes Master-Zertifikat verwenden** und wählen Sie die Zertifkatsdatei aus. Anschließend geben Sie das Kennwort für den Zugriff auf das in der Datei enthaltene Zertifikat ein.
   Wenn Sie ein neues selbst-signiertes Zertifikat erstellen wollen, wählen Sie die Option **Neues Master-Zertifikat erstellen**.
3. Geben Sie im folgenden Dialog die Angaben für das Zertifikat vollständig ein.
4. Nun wird das Zertifikat in der DriveLock Datenbank gespeichert. Klicken Sie auf **Fertigstellen**, wenn das Speichern des Zertifikates erfolgreich beendet wurde. Sofern dabei ein Fehler aufgetreten ist, erhalten Sie statt der Erfolgsmeldung einen entsprechenden Fehlerhinweis. Führen Sie in diesem Fall den Assistenten erneut aus.

Hinweis: Sobald Sie ein Master-Zertifikat erstellt und den Assistenten beendet haben, wird auf dem entsprechenden Server die Zertifikats- und Schlüsselverwaltung aktiviert und der DriveLock Enterprise Service neu gestartet.

6.2.2 Zertifikatsverwaltung konfigurieren

Durch die Einrichtung eines Master-Zertifikates wird die Zertifikats- und Schlüsselverwaltung des DriveLock Enterprise Services automatisch aktiviert. Sie können diese Einstellung jederzeit wieder deaktivieren bzw. aktivieren.

Ebenfalls zu den Einstellungen der Zertifikatsverwaltung gehört die Konfiguration des Systemverhaltens bei der Erzeugung und Erneuerung von Benutzerzertifikaten. Sie können hierbei zwischen den folgenden beiden Optionen wählen:

- Benutzerzertifikate werden nach dem Antrag automatisch und sofort erstellt und an den erstellenden Benutzer übertragen. (Standardeinstellung)
- Ein Administrator muss Benutzerzertifikate erst genehmigen, bevor der Benutzer das von ihm beantragte Zertifikat verwenden kann.

Um die Einstellungen der Zertifikatsverwaltung zu ändern, gehen Sie wie folgt vor:

1. Öffnen Sie DriveLock Enterprise Services / Doppel-Klick <Mandantenname> / Zertifikatsverwaltung.
2. Um die Zertifikatsverwaltung zu aktivieren, markieren Sie die Option **Zertifikats- und Schlüsselverwaltung aktivieren**.

3. Sollen alle Benutzerzertifikate zunächst durch den Administrator geprüft und freigegeben werden, aktivieren Sie die Option **Zertifikatsanfragen müssen vom Administrator manuell genehmigt werden**.
4. Stellen Sie die Gültigkeitsdauer der Benutzerzertifikate auf den gewünschten Wert (in Jahren) ein.
5. Klicken Sie auf Übernehmen, um die Einstellungen zu speichern.

6.3 Einstellungen in Richtlinien

Die Einstellungen für die Ver- und Entschlüsselung von Dateien und das Verhalten von DriveLock File Protection auf dem Client-Computer werden im DriveLock Richtlinien Editor vorgenommen.

Hier können Sie die folgenden Einstellungen setzen:

- Einstellungen zur Verschlüsselung konfigurieren
- Benutzeroberfläche der Verschlüsselung konfigurieren
- Einstellungen für verschlüsselte Laufwerke konfigurieren
- Zusätzliche Einstellungen konfigurieren
- Wiederherstellungszertifikat erzeugen
- Erzwungene Verschlüsselung verwenden
- Verwendetes Verschlüsselungsformat angeben

6.3.1 Einstellungen zur Verschlüsselung konfigurieren

Um die Verschlüsselungseinstellungen zu konfigurieren, klicken Sie auf den Knoten **File Protection** und anschließend auf **Einstellungen**.

Hier stehen folgende Optionen zur Auswahl:

- **Verschlüsselungsalgorithmus für verschlüsselte Ordner**: Hier legen Sie den Algorithmus fest, der für die Ver- und Entschlüsselung verwendet wird (siehe Unterstützte Verschlüsselungsverfahren).
- **Hash-Algorithmus für Passwörter bei verschlüsselten Ordnern**: Hier legen Sie den Algorithmus fest, der für die Erzeugung der Passwort-Hashes verwendet wird.
- **Minimale Passwort-Komplexität für verschlüsselte Ordner**: Die minimal erforderliche Passwortkomplexität für verschlüsselte Laufwerke sollte so definiert werden, dass sie den Firmenrichtlinien entspricht. Die Komplexität wird auf Basis der verwendeten Zeichen sowie der Passwortlänge berechnet. Wenn Sie Ihre eigene

Passwortkomplexitäts-Richtlinie erstellen möchten, wählen Sie „Richtlinie für Passwort-Komplexität“ aus und konfigurieren anschließen diese.

- **Kennwort-Richtlinie**: Sofern Ihre Richtlinien es erfordern, dass Zeichen verwendet werden sollen, die sowohl eine Zahl also auch ein Sonderzeichen sein dürfen, aktivieren Sie die Option **Ziffern als Sonderzeichen behandeln** und geben Sie die Anzahl der benötigten Zeichen an.
  Ein Wörterbuch kann entweder ein Wörterbuch-Datei aus OpenOffice sein oder eine normale Textdatei, die pro Zeile ein Wort enthält. DriveLock wird mit OpenOffice Wörterbüchern für die vier folgenden Sprachen ausgeliefert: Englisch, Deutsch, Niederländisch und Französisch. Sie können die DIZ-Dateien in dem DriveLock Installationsordner finden, auf dem Client, auf dem die DriveLock Management Konsole installiert wurde (z.B. „DictGerman.diz“).

  Achtung: Wenn Sie die Datei aus dem Dateisystem auswählen, stellen Sie sicher, dass sich die Datei auf allen Agenten Computern an exakt der gleichen Stelle befindet, da der Agent an dem angegebenen Ort sucht.

  Sie können die Datei auch dem Richtliniendateispeicher hinzufügen. Wählen Sie dazu „Richtliniendateispeicher…“ und die entsprechende Datei aus. Dateien im Richtliniendateispeicher werden Anhand eines Sterns („*“) am Anfang des Dateinamens identifiziert und werden automatisch auf den Client kopiert.

  Achtung: Wenn Sie das Wörterbuch verwenden um Passwörter zu überprüfen, beachten Sie dass auch Passwörter verweigert werden, indem ein Teil des Passwortes im Wörterbuch vorkommt (z.B.: das Wörterbuch enthält „es“, Passwörter wie „Essen“, „vergessen“ oder „Sessel“ werden nicht erlaubt).

6.3.2 Benutzeroberfläche der Verschlüsselung konfigurieren

Um die Einstellungen für die Benutzeroberfläche der Verschlüsselung zu konfigurieren, stehen Ihnen folgende Optionen zur Verfügung:

- **Verfügbare Kontext-Menüs im Windows Explorer**: Um die verfügbaren Kontextmenü-Einträge festzulegen, die ein Benutzer nach einem Rechts-Klick auf ein verschlüsseltes Verzeichnis angezeigt bekommt, klicken Sie auf Einstellen auf festen Wert und wählen Sie aus den drei Optionen aus. Ist Nicht konfiguriert ausgewählt, werden alle Einträge angezeigt.
- **Konfiguration der Start-Menü-Einträge**: Um die Ebene der verfügbaren Startmenü-Einträge festzulegen, die ein Benutzer nach einem Klick auf das Windows Start-

Symbol angezeigt bekommt, klicken Sie auf Einstellen auf festen Wert und wählen Sie aus den Optionen aus. Ist Nicht konfiguriert ausgewählt, werden die Einträge unter Alle Programme / DriveLock File Protection angezeigt.

- **Verfügbare Start-Menü-Einträge**: Um die verfügbaren Startmenü-Einträge festzulegen, die ein Benutzer nach einem Klick auf das Windows Start-Symbol angezeigt bekommt, klicken Sie auf Einstellen auf festen Wert und wählen Sie aus den Optionen aus. Ist Nicht konfiguriert ausgewählt, werden alle Einträge angezeigt.
- **Verfügbare Menü-Einträge beim Taskbar-Symbol**: Um die verfügbaren Tasksymbol-Menüeinträge festzulegen, die ein Benutzer nach einem Rechts-Klick auf das DriveLock Taskleisten-Symbol angezeigt bekommt, klicken Sie auf Einstellen auf festen Wert und wählen Sie aus den Optionen aus. Ist Nicht konfiguriert ausgewählt, werden alle Einträge angezeigt.
- **Reihenfolge der Menü-Einträge beim Taskbar-Symbol**: Um die Reihenfolge verfügbaren Tasksymbol-Menüeinträge festzulegen, die ein Benutzer nach einem Rechts-Klick auf das DriveLock Taskleisten-Symbol angezeigt bekommt, klicken Sie auf Einstellen auf festen Wert. Wählen Sie einen Eintrag aus und klicken Sie auf Nach oben oder Nach unten, um den ausgewählten Eintrag zu verschieben. Wählen Sie einen Eintrag aus und klicken Sie auf Entfernen, um einen Eintrag zu löschen. Um eine Trennlinie hinzuzufügen, wählen Sie einen Eintrag aus und klicken Sie auf Hinzuf.. Ist Nicht konfiguriert ausgewählt, werden alle Einträge in einer Standardreihenfolge angezeigt.
- **Endbenutzer-Kontaktinformationen für Offline-Wiederherstellung**: Um den Text festzulegen, die ein Benutzer nach einem Rechts-Klick auf das DriveLock Taskleisten-Symbol und der Auswahl der Option "Verschlüsselten Ordner wiederherstellen" angezeigt bekommt, klicken Sie auf Einstellen auf festen Wert und geben Sie den gewünschten Text in das Textfeld ein. Ist Nicht konfiguriert ausgewählt, wird kein Text angezeigt.
- **Format von Benutzeranzeigenamen**: Um das Format der Benutzerliste festzulegen, die ein Benutzer bei der Verwaltung berechtigter Benutzer angezeigt bekommt, klicken Sie auf Einstellen auf festen Wert und wählen Sie aus den Optionen aus. Ist Nicht konfiguriert ausgewählt, werden die Benutzer im Format [Nachname], [Vorname] angezeigt.
- **Keine Nachrichten für automatisch verbundene verschlüsselte Ordner anzeigen**: Um die Anzeige von Popup-Meldungen durch DriveLock beim automatischen Verbinden verschlüsselter Laufwerke zu unterdrücken, aktivieren Sie die Option Aktiviert. Ist Nicht konfiguriert oder Deaktiviert ausgewählt, werden Popup-Fenster angezeigt.

- **Optionen zum Speichern von Kennwörtern verschlüsselter Ordner**: Hier stellen Sie ein, ob und wie Benutzer ihr Kennwort beim Öffnen verschlüsselter Ordner speichern dürfen. Sie können Speichern verbieten, zulassen oder nur für die aktive Sitzung zulassen. Wenn Sie für aktive Sitzung auswählen, wird das Passwort gelöscht, sobald sich der Benutzer abmeldet, gilt dafür aber für alle verschlüsselten Ordner, die mit dem selben Passwort geschützt sind. Damit erleichtern Sie Anwendern das Arbeiten mit mehreren verschlüsselten Ordner bei trotzdem hoher Sicherheit.

6.3.3 Einstellungen für verschlüsselte Laufwerke konfigurieren

Um die Einstellungen für verschlüsselte Laufwerke zu konfigurieren, stehen Ihnen folgende Optionen zur Verfügung:

- **Verfügbare Wiederherstellungsverfahren für verschlüsselte Ordner**: Um festzulegen welche Wiederherstellungsoptionen einem Benutzer zur Verfügung stehen, klicken Sie auf Einstellen auf festen Wert und wählen Sie aus den Optionen aus. Ist Nicht konfiguriert ausgewählt, werden alle Optionen angezeigt.
- **Intervall zwischen Überprüfungen auf Zertifikatswiederruf**: Um den Zeitraum festzulegen, innerhalb dessen keine erneute Überprüfung des Benutzerzertifikates auf einen erfolgten Rückruf desselben erfolgt, klicken Sie auf Einstellen auf festen Wert und wählen Sie aus den Optionen aus. Ist Nicht konfiguriert ausgewählt, beträgt das Intervall 24 Stunden.
- **Zugriff auf Dateien in verschlüsselten Ordnern**: Um festzulegen, wie sich DriveLock File Protection verhalten soll, wenn ein Benutzer keine Berechtigung zur Ver-/Entschlüsselung hat, klicken Sie auf Einstellen auf festen Wert und wählen Sie aus den Optionen aus. Ist Nicht konfiguriert ausgewählt, wird der Zugriff auf das Verzeichnis verweigert. Folgende Optionen stehen zur Auswahl und verhalten sich wie folgt:
  - **Verweigern**: Benutzer ohne Berechtigungen können nicht auf das Verzeichnis zugreifen, auch wenn Sie entsprechende Windows-Berechtigungen hätten. Er erscheint die Windows-Meldung "Zugriff verweigert".
  - **Erlauben für Administratoren**: Benutzer ohne Berechtigungen können nur darauf zugreifen, wenn Sie der Gruppe der Administratoren

Achtung: Wird der Zugriff ohne Berechtigungen ermöglicht, verhält sich das Verzeichnis wie ein ganz normales Windows-Verzeichnis, d.h. Dateien werden beim Öffnen nicht entschlüsselt, beim Schreiben aber auch nicht verschlüsselt. Bei berechtigten Benutzern geht DriveLock File Protection aber innerhalb eines verschlüsselten Verzeichnisses immer von einer verschlüsselten Datei aus und würde auch eine unverschlüsselte Datei entschlüsseln, was dazu führt, dass ein

berechtigter Benutzer mit dieser Datei nichts anfangen kann und diese ggf. beim Schreiben komplett unbrauchbar macht.

- **Automatisches Verbinden von verschlüsselten Ordnern**: Um festzulegen, wie sich DriveLock File Protection beim Verbinden verschlüsselter Laufwerke verhalten soll, klicken Sie auf Einstellen auf festen Wert und wählen Sie aus den Optionen aus. Ist Nicht konfiguriert ausgewählt, gilt die Option An (Dialog bei Bedarf anzeigen). Folgende Optionen stehen zur Auswahl und verhalten sich wie folgt:
  - **An** (Dialog bei Bedarf anzeigen): DriveLock File Protection versucht, den Ordner mit Hilfe des im Zertifikatsspeicher vorhandenen Benutzerzertifikats oder mit einem zuvor gespeicherten Passwort zu verbinden. Hat der Benutzer keine Berechtigung oder stimmt das Passwort nicht, öffnet sich ein Fenster und der Benutzer kann eine Authentisierungsmethode auswählen. Diese Option ist sinnvoll, wenn Passwörter nicht gespeichert werden dürfen, oder Benutzerzertifikate nicht im Zertifikatsspeicher von Windows sondern auf externen Medien wie z.B. Smartcards oder Token gespeichert sind.
  - **Nur vollautomatisch, keine Dialoge anzeigen**: DriveLock File Protection versucht, den Ordner mit Hilfe des im Zertifikatsspeicher vorhandenen Benutzerzertifikats oder mit einem zuvor gespeicherten Passwort zu verbinden. Hat der Benutzer keine Berechtigung oder stimmt das Passwort nicht, wird der Benutzer als nicht berechtigt angesehen.
  - **Aus**: Es erfolgt keine automatische Verbindung mit einem verschlüsselten Verzeichnis. Der Benutzer wird solang als unberechtigter Benutzer angesehen, bis er einen Rechts-Klick auf das Verzeichnis durchführt und den Menüeintrag Verschlüsselten Ordner verbinden auswählt.

6.3.4 Zusätzliche Einstellungen konfigurieren

Folgende zusätzliche Optionen sind verfügbar:

- **Dateien und Ordner, die von der automatischen Verbindung ausgenommen sind**: Um Verzeichnisse festzulegen, bei denen DriveLock keinen Versuch einer automatischen Verbindung unternehmen soll, klicken Sie auf Einstellen auf feste Liste und bearbeiten Sie die Liste der gewünschten Verzeichnisse oder Dateien mit Hilfe der Schaltflächen Hinzufügen, Löschen und Bearbeiten.
- **Namen von Backup-Programmen (mit Zugriff nur auf verschlüsselte Dateien)**: Um Programme festzulegen, welche auch ohne Berechtigung Zugriff auf verschlüsselte Verzeichnisse haben müssen, klicken Sie auf Einstellen auf feste Liste und

bearbeiten Sie die Liste der gewünschten Programme mit Hilfe der Schaltflächen Hinzufügen, Löschen und Bearbeiten. Geben Sie dabei den kompletten Programmnamen ohne Pfad an, (z.B. backup.exe). Standardmäßig werden bereits die Programme von Dropbox, OneDrive und Google Drive berücksichtigt.

Hinweis: Lange Dateinamen werden vom Treiber nicht unterstützt um Backup-Programme zu erkennen. Geben Sie stattdessen die ersten sieben Zeichen an, z.B. BACKUP.EXE aber MYBACKU für MyBackupBackupAndRestore.exe.

6.3.5 Verwendetes Verschlüsselungsformat

Auf dem neuen Format für verschlüsselte Dateien baut die zukünftige Entwicklung für die DriveLock File Protection auf.

Mit dieser Einstellung können Sie sich aktiv zwischen dem alten oder dem neuen Format für Ihre DriveLock Agenten entscheiden. Wenn Sie den DriveLock Agenten auf Ihren Clients neu installieren und File Protection aktivieren, wird automatisch das neue Format verwendet. Wenn Sie bereits File Protection auf Ihren Agenten eingesetzt haben und dort auch schon Ordner verschlüsselt sind, sollten Sie das alte Format weiterverwenden.

Hinweis: Beachten Sie bitte, dass Sie die beiden Formate in separaten Richtlinien zuweisen, da diese nicht kompatibel sind.

Folgende Optionen stehen als fest einstellbare Werte zur Verfügung:

- **Automatisch (Standard)**:
  Je nach vorhandener Version auf den Agenten verwendet DriveLock entweder das neue oder das alte Format.
- **Neues Format**:
  Verwenden Sie diese Option, wenn keine Kompatibilität mit verschlüsselten Ordnern im alten Format erforderlich ist.
- **Altes Format**:
  Wenn auf Ihren Agenten bereits verschlüsselte Ordner aus älteren DriveLock-Versionen vorhanden sind, empfehlen wir diese Option.
- **Neues Format (reduzierte Funktionalität)**:
  Diese Option schränkt das neue Format ein, beispielsweise funktioniert das Verstecken von Dateien in diesem Fall nicht. Außerdem ist das Mounten bei Zugriff auf verschlüsselte Ordner nicht möglich. Verwenden Sie diese Option nur wenn Sie Probleme mit dem neuen Format haben.

- **Altes Format (alter Treiber)**:
  Falls es sich bei Ihren Agenten um Clients handelt, auf denen noch Windows XP läuft, wird diese Option automatisch verwendet. Ansonsten handelt es sich um eine Fall-back-Option, falls Kompatibilitätsprobleme beim alten Treiber auftreten sollten.

Achtung: Bitte beachten Sie, dass das Kombinieren der verschiedenen Verschlüsselungsmethoden zu einer Beschädigung der Daten führen kann, z. B. wenn "Altes Format (alter Treiber)" aktiv ist, obwohl mit dem "Neuen Format" erstellte Ordner vorhanden sind. Auf diese Ordner sollte (mit dem alten Treiber) nicht zugegriffen werden.

Die beiden unteren Einstelllungen bieten lediglich Ausweichmöglichkeiten.

Hinweis: Beachten Sie bitte auch, dass die Verschlüsselungsformate **Altes Format** und **Altes Format (alter Treiber)** das Distributed File System (DFS) nicht unterstützen.

6.4 Erzwungene Verschlüsselung

Für die erzwungene Verschlüsselung von externen Datenträgern können Sie statt der Container Verschlüsselung (siehe DriveLock Encryption 2-Go) auch die Dateiverschlüsselung verwenden. Bei großen Datenträgern beschleunigt das die Initialisierung deutlich, weil nicht erst ein Container angelegt werden muss, sondern nur die zu kopierenden Dateien verschlüsselt werden. Außerdem können sie so mehrere Ordner mit unterschiedlichen Berechtigungen anlegen lassen, z.B. einen Ordner mit Unternehmenszertifikat, auf den alle Zertifikatsinhaber transparent zugreifen können, einen Ordner mit Benutzername und Passwort nur für den Besitzer und einen Ordner für unverschlüsselte Daten.

Erzwungene Verschlüsselung mit DriveLock File Protection verwenden

1. Aktivieren sie die erzwungene Verschlüsselung mit DriveLock File Protection in der Richtlinie unter:
   Verschlüsselung/ Einstellungen / **Methode für die erzwungene Verschlüsselung von Wechseldatenträgern**
   Selektieren Sie **DriveLock File Protection**. Damit wird für alle neuen unverschlüsselten Laufwerke, für die in einer Regel die erzwungene Verschlüsselung aktiviert ist, die Datei- und Ordner basierte Verschlüsselung verwendet.
   Wollen Sie Ihre Benutzer zwischen Container-basierte oder die Datei- und Order basierte Verschlüsselung auswählen lassen, markieren Sie **Entscheidung durch den Benutzer**.

2. Konfigurieren Sie die Verschlüsselungseinstellungen im Unterknoten **Erzwungene Verschlüsselung**.
   Öffnen Sie das Kontextmenü, wählen dann **Neu** und legen anschließend eine oder ggf. mehrere neue Verschlüsselungsregeln für unterschiedliche Benutzergruppen an.
   a. Im Konfigurationsdialog für die Regel erstellen Sie unter **Allgemein** eine kurze Beschreibung für die Regel.
   b. Im Reiter **Dateisystem** konfigurieren Sie, ob bestehende Daten erhalten bleiben sollen und in den konfigurierten Ordner verschoben/verschlüsselt werden sollen und legen fest ob die Mobile Encryption Anwendung auf das Laufwerk kopiert werden soll. Wenn Sie bestehende Daten erhalten hier nicht auswählen, werden alle vorhandenen Daten gelöscht, bevor der Stick verschlüsselt wird.
   c. Im Reiter **Einstellungen** legen Sie die Art der Berechtigungen und der Verschlüsselung fest und vergeben einen Namen für den verschlüsselten Ordner. Unter **Erweiterte Einstellungen** können sie die Namen für weitere Ordner vergeben und festlegen, ob diese stattdessen bei der Initialisierung die vorhandenen unverschlüsselten Daten aufnehmen sollen.
   d. In den Reitern **Computer**, **Netzwerke** und **Angemeldete Benutzer** legen Sie fest, für wen und wo die Regel gelten soll.
   e. Legen Sie die **Priorität** fest mit der die Regel angewendet werden soll. Es wird immer die zutreffende Regel mit der höchsten Priorität verwendet.

Benutzerauswahl der Verschlüsselungsregel (Optional)

Analog erstellen Sie neue Benutzerauswahlregeln und fügen dort Verschlüsselungsregeln hinzu, wenn Anwender selbst eine geeignete Verschlüsselungsregel auswählen sollen. Hier müssen Sie die Priorität so festlegen dass die Regel vor den Verschlüsselungsregeln zur Anwendung kommt.

> Hinweis: Haben Sie Entscheidung durch den Benutzer konfiguriert, erscheint zuerst der Auswahldialog für die Verschlüsselungsmethode und dann der Dialog mit den Benutzerauswahlregeln. Achten sie darauf, die in beiden Dialogen verfügbaren Optionen nur einmal zu markieren.

6.5 Wiederherstellung verschlüsselter Laufwerke konfigurieren

Damit Sie die Funktionalität der Offline-Passwort-Wiederherstellung nutzen können, müssen Sie vor der Erstellung des ersten verschlüsselten Verzeichnisses ein Hauptzertifikat bestehend aus einem öffentlichen und privaten Schlüsselpaares erzeugen. Hierzu können

durchaus auch mehrere Zertifikate angelegt werden, die über Computer / Netzwerke / Angemeldete Benutzer gefiltert werden können. Dies ist dann sinnvoll, wenn sich der Benutzerkreis unterscheidet, die eine Wiederherstellung verschlüsselter Daten durchführen dürfen. Es sollte aber mindestens das Standard-Wiederherstellungszertifikat mit der Priorität Niedrigste erzeugt werden.

> Beispiel: Gerade in großen Umgebungen kann es bevorzugt werden, ein Standard-Zertifikat zu erstellen, welches für alle verwendet wird. Lediglich für den Vorstand gibt es ein eigenes Wiederherstellungszertifikat. Das Standard-Zertifikat erhält der IT-Helpdesk, damit für alle Mitarbeiter außer dem Vorstand, das Passwort von verschlüsselten Verzeichnisse zurückgesetzt werden kann. Nur der IT-Sicherheitsbeauftragte und der IT-Enterprise Administrator erhalten das Wiederherstellungszertifikat des Vorstands, damit auch hier eine Wiederherstellung möglich ist. Mit dieser Maßnahme wurde der Kreis der Personen, die potentiell Zugriff auf vertrauliche Daten haben (die des Vorstands), weiter eingeschränkt.

Um die Einstellungen für die Wiederherstellung verschlüsselter Laufwerke zu konfigurieren, öffnen Sie im Knoten **File Protection** den Unterknoten **Wiederherstellung verschlüsselter Ordner**.

> Hinweis: Bei der Wiederherstellung verschlüsselter Verzeichnisse muss dann das passende Wiederherstellungs-Zertifikat ausgewählt werden, wenn Zertifikate mit mehreren Prioritäten erstellt wurden.

Standardmäßig ist zunächst ein Zertifikatseintrag vorhanden, welcher für alle verschlüsselte Verzeichnisse verwendet wird (sofern konfiguriert). Dieses Zertifikat hat die Priorität **Niedrigste** und kann nicht gelöscht werden.

Um ein Standard-Wiederherstellungszertifikat zu erstellen, führen Sie folgende Schritte durch:

- Doppelklicken Sie auf **Zertifikatsbasierte Wiederherstellung (Priorität Niedrigste)**.
- Klicken Sie auf **Zertifikatsdatei** und wählen Sie **Neu anlegen** aus dem Drop-Down Menu aus. Dadurch wird der Assistent für die Erzeugung des Hauptzertifikates gestartet.
- Geben Sie anschließend entweder den Ordner an, wo Sie die Zertifikatsdatei abspeichern möchten oder wählen Sie alternativ eine Smartcard als Speicherort.

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

Achtung: Stellen Sie sicher, dass diese Datei an einem sicheren Ort abgespeichert wird, da sie für die Passwort-Wiederherstellung dringend benötigt wird.

- Geben Sie nun das Passwort für den Zugriff auf den privaten Schlüsselbereich des Zertifikates an. Sie müssen das Passwort aus Sicherheitsgründen zweifach eingeben.
- Um Fortzufahren, klicken Sie auf Weiter. Es dauert einige Sekunden, um das Hauptzertifikat zu erzeugen. Anschließend werden Sie benachrichtigt, wenn der Prozess abgeschlossen ist und die Datei an dem zuvor angegebenen Ort abgespeichert wurde.

Achtung: Stellen Sie sicher, dieses Passwort nicht zu vergessen. Sie sollten dieses ebenso an einem anderen sicheren Ort aufbewahren (z.B. in einem Tresor).

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

Die soeben erzeugte Zertifikatsdatei wird nun angezeigt.

Achtung: Sobald das Zertifikat erzeugt und der erste verschlüsselte Container erstellt wurde, darf kein neues Zertifikat mehr erstellt werden, da das alte damit überschrieben wird und somit für eine Wiederherstellung nicht mehr verwendet werden kann.

Wenn Sie auf **Eigenschaften** klicken, erhalten Sie zusätzliche Informationen über das Hauptzertifikat.

Das Zertifikat wird ebenfalls in dem privaten Zertifikatsspeichers des aktuellen Benutzers gespeichert. Der öffentliche Schlüssel des Zertifikates wird auch innerhalb des lokalen Richtliniendateispeichers abgelegt.

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

Wenn Sie bisher schon ohne ein Hauptzertifikat verschlüsselte Verzeichnisse verwendet haben, ist es sinnvoll, die Option **Wiederherstellungsinformationen zu bestehenden**

Ordnern hinzufügen zu aktivieren. In diesem Fall überprüft DriveLock jedes Mal wenn ein Verzeichnis verbunden wird, ob bereits eine Wiederherstellungsinformation vorhanden ist und erzeugt gegebenenfalls diese Information. Anschließend werden die zur Wiederherstellung nötigen Daten auch an den DriveLock Enterprise Service übertragen.

Sofern der DriveLock Enterprise Service in Ihrer Umgebung nicht verwendet wird oder Sie die Übertragung der Wiederherstellungsdaten an den DriveLock Enterprise Service nicht möchten, können Sie dieses Verhalten durch Aktivieren der Option **Keine Offline-Wiederherstellung – Daten nicht an DES hochladen** verhindern.

Rechtsklicken Sie auf **Wiederherstellung verschlüsselter Ordner** und wählen **Neu** -> **Wiederherstellungs-Regel** aus dem Kontextmenü, um ein weiteres Zertifikat zu erzeugen.

Am Anfang ist hier noch keine Zertifikatsdatei angegeben. Klicken Sie auf **Zertifikatsdatei** und wählen Sie **Neu anlegen** aus dem Drop-Down Menu aus.

Dadurch wird wieder der Assistent für die Erzeugung des Hauptzertifikates gestartet. Der Ablauf ist nun der gleiche wie bei der Erzeugung des Zertifikates für die niedrigste Priorität.

Über Einstellungen auf den Reitern **Computer**, **Netzwerke** und **Angemeldete Benutzer** können Sie nun festlegen, für welche der gleichnamigen Bereiche dieses Zertifikat verwendet werden soll. Die Funktionsweise ist dabei die gleiche wie auch an vielen anderen Stellen bei DriveLock und wird daher hier nicht detaillierter beschrieben.

Das neue Zertifikat wird anschließend in der Detailansicht rechts angezeigt.

Das erste zusätzliche Zertifikat erhält dabei die Priorität 1, jedes weitere eine um eins erhöhte Priorität als die höchste vorhandene.

Rechts-klicken Sie auf einen Eintrag und wählen Sie **Nach unten** oder **Nach oben**, um die Reihenfolge der Priorisierung anzupassen. Über **Löschen** können Sie ein vorhandenes Zertifikat löschen.

Achtung: Wenn Sie ein bereits verwendetes Zertifikat löschen, ist darüber keine Wiederherstellung mehr möglich.

6.5.1 Unternehmenszertifikat

Verschlüsselte Ordner mit einem Unternehmenszertifikat können von jedem Anwender verbunden werden, der Zugriff auf den zugehörigen privaten Schlüssel im Windows Zertifikats-Speicher hat. In dem Fall prüfte DriveLock beim Verbinden eines verschlüsselten Ordners als erstes, ob es den Ordner mit dem Unternehmenszertifikat entschlüsseln kann und der

Ordner wird ohne weitere Benutzereingaben verbunden. Andernfalls wird der Benutzer nach seinen Zugangsdaten gefragt.

DriveLock erstellt die Unternehmenszertifikate nicht - Sie können den öffentlichen Schlüssel eines Zertifikat (*.cer), das Sie besitzen, hinzufügen. Den privaten Schlüssel (*.pfx) müssen Sie selbst im Windows Zertifikats-Speicher (Benutzer- oder Computerkonto) hinterlegen.

Technisch sind Unternehmenszertifikat und Wiederherstellungszertifikat sehr ähnlich und werden auf die selbe Art konfiguriert.

So erstellen Sie ein Unternehmenszertifikat:

- Öffnen Sie im Knoten **File Protection** den Unterknoten **Wiederherstellung verschlüsselter Ordner**, wählen dann **Neu** und **Unternehmenszertifikat**. Auf dem Reiter Allgemein erstellen Sie eine Beschreibung und importieren ein Zertifikat.
- Markieren Sie **Aktiviert** um das Zertifikat beim Erstellen / Aktualisieren von Ordnern zu verwenden.
- Im Reiter **Optionen** markieren Sie die gewünschte Art der Verwendung.

Hinweis: Zum Ausprobieren können Sie z.B. ein Wiederherstellungszertifikat als Unternehmenszertifikat verwenden.
Importieren Sie DLFfeRecovery.cer in die Richtline und DLFfeRecovery.pfx in den Windows Zertifikats-Speicher.

Unternehmenszertifikat erneuern

DriveLock kümmert sich nicht um das Ablaufdatum eines Unternehmenszertifikats, Sie können damit weiterhin verschlüsselte Ordner erstellen und verbinden. Jedoch können Sie jederzeit neue Unternehmenszertifikate zur Richtlinie hinzufügen und abgelaufenen Zertifikate aus der Richtlinie entfernen.

Hinweis: Wenn Sie ein Unternehmenszertifikat aus dem Windows Zertifikats-Speicher löschen, können Sie mit diesem Schlüssel den verschlüsselten Ordner nicht mehr verbinden. Wenn das der einzige Schlüssel für den Ordner war kann eine neues Unternehmenszertifikat nicht mehr hinzugefügt werden.

6.6 Benutzer und Zertifikate verwalten

Bevor Benutzer und Zertifikate in DriveLock File Protection verwaltet werden können, müssen Sie einige Einstellungen konfigurieren. Diese sind unter Master-Zertifikat für die Schlüsselverwaltung einrichten und Zertifikatsverwaltung konfigurieren beschrieben.

6.6.1 Wie funktioniert die Benutzerverwaltung?

Die Benutzerverwaltung in DriveLock File Protection hilft Ihnen, ohne eine bereits vorhandene Public-Key-Infrastruktur (PKI) Benutzer und deren zugehörige Zertifikate zu verwalten.

Die integrierte Benutzerverwaltung wird nicht benötigt, wenn

- Sie bereits eine Microsoft Active Directory Umgebung haben, in denen auch Benutzerzertifikate verwaltet werden
- Sie eine andere PKI im Einsatz haben, die mit Microsoft Windows kompatibel ist
- Sie ausschließlich mit Passwörtern (nicht Windows-Passwörter) als Authentifizierung arbeiten möchten

Der große Vorteil, Benutzerzertifikate als Authentisierungshilfsmittel für die DriveLock File Protection zu verwenden, liegt darin, dass damit eine vollkommen transparente Ver- und Entschlüsselung ermöglicht wird, ein Benutzer nichts davon merkt und somit in keinster Weise in seiner üblicher Arbeitsweise beeinträchtigt wird. Bei jedem Zugriff auf ein verschlüsseltes Verzeichnis prüft DriveLock File Protection, ob im Zertifikatsspeicher des Benutzers ein Benutzerzertifikat vorhanden ist und dieses für die automatische Authentifizierung verwendet werden kann.

Damit Sie sich nicht mit dem Thema PKI auseinandersetzen müssen, sind alle für eine einfache, schnelle und übersichtliche Verwaltung von Benutzern und deren Zertifikate notwendigen Funktionen in DriveLock File Protection bereits integriert. Benutzer können selbst Zertifikate beantragen, beantragte Zertifikate können automatisch genehmigt, erstellt und im Benutzerzertifikatsspeicher des Betriebssystems abgelegt werden. Sie als IT-Administrator können Benutzer hinzufügen, bearbeiten und löschen, können Zertifikate ändern, zurücknehmen, löschen und aus dem Active Directory oder von Datei oder anderem Medium hinzufügen.

Hinweis: Zwischen einem Benutzer und einem Zertifikat besteht in DriveLock File Protection eine enge Beziehung. So wie es keinen Benutzer ohne Zertifikat geben kann, kann es kein Zertifikat ohne einen dazu gehörenden Benutzer geben. Beide bilden also eine Einheit. Beantragt ein Benutzer ein Zertifikat, legt DriveLock automatisch auch einen entsprechenden Benutzer an. Ebenso können Sie als IT-Administrator keinen Benutzer anlegen, ohne ein passendes Zertifikat zu haben.

Achtung: Die DriveLock PKI speichert und verwaltet nicht die privaten Schlüssel der Benutzerzertifikate. Anwender müssen ihr Zertifikat mit privatem Schlüssel (PFX-

Datei) mit der DriveLock Anwendung aus dem Windows Zertifikatsspeicher exportieren und sicher aufbewahren. Sie müssen das Zertifikat wieder in den Windows Zertifikatsspeicher importieren um auf ihre verschlüsselten Ordner von einem anderen Computer zuzugreifen.

6.6.2 Benutzer verwalten

Die Benutzer werden mit Hilfe der DriveLock Management Konsole verwaltet. Sie gelangen zur DriveLock File Protection Benutzerverwaltung, in dem Sie im Navigationsbereich auf **DriveLock File Protection** und dann auf **Benutzer und Gruppen** klicken.

Die rechte Seite zeigt Ihnen eine Übersicht über alle in der DriveLock Datenbank gespeicherten Benutzer bzw. Gruppen an.

Achtung: Bitte beachten Sie, dass Sie als Administrator mit Hilfe dieser Benutzerverwaltung keine Zertifikate erzeugen können. Sie können hier lediglich bestehende Zertifikate einer PKI importieren, zu denen dann auch der entsprechende Benutzer angelegt wird. DriveLock File Protection Zertifikate erzeugen kann nur ein Benutzer selbst. Wie das funktioniert, ist im DriveLock Benutzerhandbuch beschrieben.

Um einen Benutzer oder eine Gruppe mit einem vorhandenen Zertifikat anzulegen (d.h. ein Zertifikat zu importieren), führen Sie folgende Schritte durch:

1. Rechtsklicken Sie auf **Benutzer und Gruppen** im Navigationsbereich oder auf eine leere Stelle in der Detailansicht rechts
2. Im Kontextmenü klicken Sie auf **Neu** und wählen entweder
   - **Benutzer aus Active Directory...**, wenn Sie aus dem Microsoft AD einen Benutzer mit vorhandenem Zertifikat auswählen möchten. In diesem Fall erscheint der Standarddialog zu Auswahl von Objekten aus dem Active Directory und Sie können einen Benutzer auswählen.
   - **Benutzer von Zertifikat...**, wenn Sie ein Zertifikat in Form eine Zertifikatsdatei (*.cer) vorliegen haben. In diesem Fall können Sie diese Zertifikatsdatei über den Dateiauswahldialog öffnen.
3. Nach dem Einlesen des Zertifikates öffnet sich das Eigenschaften-Fenster des Benutzers
4. Sofern aus dem Zertifikat die Daten bereits ausgelesen werden konnten, sind die passenden Eingabefelder bereits mit diesen Werten gefüllt. Bitte tragen Sie fehlende Informationen wie z.B. E-Mail-Adresse oder Abteilung ein.

5. Optional: In Umgebungen mit mehr als einem DES und verschiedenen Mandanten, kann der neue Benutzer für einen bestimmten Mandanten angelegt werden. Wählen Sie in diesem Fall aus der Dropdown-Liste Mandant den richtigen Mandant aus. Belassen Sie ansonsten diesen Eintrag unverändert.
6. Optional: Sie können auch ein beliebiges Anzeigebild aus einer Grafikdatei hinzufügen. Da dieses Bild an verschiedenen Stellen bei der Benutzerauswahl angezeigt wird, kann es die Auswahl des richtigen Benutzers insbesondere bei gleichen Namen erleichtern. Klicken Sie dazu auf Anzeigebild ändern und wählen Sie eine passende Grafikdatei aus. Klicken Sie auf Öffnen. Konnte die Datei als Anzeigebild verwendet werden, wird dieses neue Bild nun links oben bei den Benutzereigenschaften angezeigt.
7. Klicken Sie auf OK, um den Benutzer anzulegen und die Änderungen zu speichern. In der Detailansicht rechts wird der neue Benutzer nun angezeigt.

Hinweis: Wenn ein Benutzer selbst ein Zertifikat beantragt/erstellt, wird automatisch ein entsprechender Benutzer angelegt.

Um die Eigenschaften eines Benutzers zu ändern oder anzusehen, doppelklicken Sie auf den gewünschten Eintrag:

- Der Reiter **Verwaltete Ordner** zeigt alle zentral verwaltete Verzeichnisse, für die dieser Benutzer Berechtigungen hat.
- Der Reiter **Zertifikate** zeigt die Zertifikate, die diesem Benutzer zugeordnet und die in der Datenbank gespeichert sind.

Um einen Benutzer zu löschen, rechtsklicken Sie auf den gewünschten Eintrag und wählen Sie Benutzer löschen aus dem Kontextmenü aus.

6.6.3 Gruppen verwalten

DriveLock File Protection Gruppen sind ein Satz von DriveLock Benutzern. DriveLock Gruppen können zu zentral verwalteten verschlüsselten Ordner zugewiesen werden. Jedes mal wenn DriveLock Benutzer zu einer DriveLock Gruppe hinzugefügt oder daraus entfernt werden, passt der DriveLock Enterprise Server im Hintergrund die korrespondierenden Benutzer bei allen zentral verwalteten Ordner an, die diese DriveLock Gruppe zugeordnet haben.

Hinweis: DriveLock Gruppen verhalten sich anders als Windows (AD) Gruppen. Für AD Gruppen werden die Berechtigungen zum Zugriffszeitpunkt geprüft. Da

Gruppen jedoch keine Zertifikate besitzen können und sich nicht authentifizieren können, muss DriveLock die entsprechenden Benutzer einzeln den jeweiligen Ordnern zuweisen. Es kann ca. 15 Minuten dauern bis diese Zuweisung abgeschlossen ist.

Um eine neue Gruppe anzulegen rechtsklicken Sie **Benutzer und Gruppen** und dann **Neu**.

Sie können entweder eine neue DriveLock Gruppe anlegen und die gewünschten DriveLock Benutzer hinzufügen oder Sie importieren eine bestehende Gruppe aus dem Group from Active Directory (AD). Beim Import aus dem AD werden die Mitglieder der AD Gruppe unter folgenden Bedingungen zur DriveLock Gruppe hinzugefügt:

- der AD Benutzer existiert bereits als DriveLock Benutzer => der Benutzer wird einfach zur DriveLock Gruppe hinzugefügt
- der AD Benutzer besitze ein gültiges Zertifikat => ein neuer DriveLock Benutzer wird erzeugt und dann zur DriveLock Gruppe hinzugefügt
- der AD Benutzer besitzt kein gültiges Zertifikat => ein Hinweis wird angezeigt und der Benutzer wird nicht hinzugefügt

Im Eigenschaften-Dialog der neuen Gruppe können Sie nun auf dem Reiter Allgemein den Gruppennamen vergeben/anpassen und den richtigen Mandanten auswählen. Auf dem Reiter Benutzer können Sie Benutzer des Mandanten hinzufügen/anpassen. Mindestens einen Benutzer müssen Sie als Gruppenadministrator markieren. Mit OK speichern Sie die neue Gruppe.

Hinweis: Sobald die Gruppe angelegt ist kann nur noch ein Gruppenadministrator mittels der DriveLock Anwendung weitere Benutzer hinzufügen und Administrator-Berechtigungen vergeben oder entziehen. Mehr dazu ist im DriveLock Benutzerhandbuch beschrieben.

Öffnen Sie den Eigenschaftendialog einer DriveLock Gruppe um Informationen zu den Gruppenmitgliedern und den zugewiesenen zentral verwalteten Ordner zu erhalten. Als DriveLock Administrator können Sie in Ausnahmefällen, falls der Gruppen-Administrator nicht verfügbar ist, Benutzer oder verwaltetet Ordern aus der Gruppe entfernen.

6.6.4 Zertifikate verwalten

Zertifikate werden in der DriveLock Management Konsole verwaltet. Sie gelangen zur DriveLock File Protection Zertifikatsverwaltung, in dem Sie im Navigationsbereich auf **DriveLock File Protection** und dann auf **Zertifikate** klicken.

Es wird zwischen den folgenden drei Kategorien unterschieden:

- **Beantragte Zertifikate**: Hier sehen Sie alle Zertifikate, die durch Benutzer beantragt oder verlängert wurden und von einem Administrator (z.B. Ihnen) noch nicht bearbeitet wurden. Ein Zertifikatsantrag kann hier entweder abgelehnt oder angenommen werden.

Hinweis: Die Genehmigung von Zertifikaten ist nur dann notwendig, wenn Sie in den Einstellungen des DES die entsprechende Option aktiviert haben. Ansonsten enthält diese Liste niemals Zertifikate.

- **Aktive Zertifikate**: Diese Übersicht zeigt alle derzeit aktiven Zertifikate, die in der DriveLock Datenbank gespeichert sind. Hier können Sie Zertifikate ansehen, den öffentlichen Teil exportieren und Zertifikate löschen oder widerrufen.
- **Widerrufene Zertifikate**: Diese Liste zeigt Ihnen alle Zertifikate, die widerrufen wurden. Durch den Widerruf wird ein Zertifikat als ungültig gekennzeichnet, aber noch nicht aus der Datenbank gelöscht. Hier können Sie widerrufene Zertifikate ansehen, den öffentlichen Teil exportieren und den Widerruf zurücknehmen (ein Zertifikat wird dann wieder als aktiv gekennzeichnet).

Klicken Sie auf eine der drei Kategorien, um sich alle zu dieser Kategorie gespeicherten Zertifikate anzeigen zu lassen.

Die rechte Seite zeigt Ihnen jeweils eine Übersicht über alle in der DriveLock Datenbank gespeicherten Zertifikate an.

Um die angezeigten Einträge nach einer anderen Spalte (Standard ist Objektname) zu sortieren, klicken Sie auf eine der Spaltenüberschriften. Um die Reihenfolge von Auf- nach Absteigend bzw. von Ab- nach Aufsteigend zu ändern, klicken Sie ein weiteres Mal auf diese Spaltenüberschrift.

Um Zertifikatsanträge zu bearbeiten, gehen Sie folgendermaßen vor:

1. Klicken Sie auf **Beantragte Zertifikate** im Navigationsbereich.
2. Rechtsklicken Sie auf den Zertifikatseintrag, den Sie bearbeiten möchten.
3. Um den Antrag zu akzeptieren und das Zertifikat auszustellen, wählen Sie im Kontextmenü **Alle Aufgaben** und **Antrag akzeptieren**. Der Listeneintrag des Zertifikats wird entfernt, das Zertifikat wird aktiviert. Wenn Sie den gestellten Zertifikatsantrag ablehnen und das Zertifikat nicht ausstellen möchten, wählen Sie **Antrag ablehnen**. Der Listeneintrag des Zertifikats wird entfernt, das Zertifikat wird gelöscht.

Um ein aktives Zertifikat zu widerrufen, führen Sie folgende Schritte aus:

1. Klicken Sie auf **Aktive Zertifikate** im Navigationsbereich.
2. Wählen Sie im Kontextmenü **Alle Aufgaben** und dann **Widerrufen...** aus.
3. Wählen Sie einen Grund für den Widerruf aus der Dropdown-Liste aus.
4. Optional: Geben Sie im Textfeld **Bemerkung** weitere Informationen zum Widerruf dieses Zertifikates ein.
5. Klicken Sie **OK**, um das Zertifikat endgültig zu widerrufen. Der Listeneintrag des Zertifikats wird entfernt, das Zertifikat wird als widerrufen markiert.

Um ein widerrufenes Zertifikat erneut zu aktivieren, führen Sie folgende Schritte aus:

1. Klicken Sie auf **Widerrufene Zertifikate** im Navigationsbereich.
2. Wählen Sie Alle Aufgaben und dann **Widerrufen aufheben** aus.
3. Klicken Sie **Ja**, um das Zertifikat zu aktivieren. Der Listeneintrag des Zertifikats wird entfernt, das Zertifikat wird aktiviert.

Um ein Zertifikat zu exportieren, führen Sie folgende Schritte aus:

1. Klicken Sie auf **Aktive** oder **Widerrufene Zertifikat**e im Navigationsbereich.
2. Wählen Sie **Zertifikat exportieren...** aus.
3. Wählen Sie ein Verzeichnis und einen Dateinamen, um den öffentlichen Bereich des Zertifikates in einer Datei (Endung .cer) zu speichern.

Hinweis: Diese Zertifikatsdatei kann von einem Benutzer verwendet werden, um den Zertifikatsbesitzer (d.h. der Benutzer von dem dieses Zertifikat generiert wurde) für ein bestimmtes privates Verzeichnis zu autorisieren. Dieser Vorgang wird im DriveLock Benutzerhandbuch beschrieben.

Um ein aktives Zertifikat zu löschen, führen Sie folgende Schritte aus:

1. Klicken Sie auf **Aktive Zertifikate** im Navigationsbereich.
2. Wählen Sie **Zertifikat löschen** aus.
3. Klicken Sie **Ja**, um das Zertifikat endgültig zu löschen. Der Listeneintrag des Zertifikats wird entfernt, das Zertifikat wird gelöscht.

Achtung: Bitte beachten Sie, dass das Löschen von Zertifikaten nicht den in der Datenbank gespeicherten Benutzer löscht. Es ist jedoch nicht mehr möglich, diesen Benutzer für den Zugriff auf ein zentral verwaltetes Verzeichnis zu autorisieren.

Bereits eingerichtete Berechtigungen bleiben davon unberührt, so lange der Benutzer sein Benutzerzertifikat im Zertifikatsspeicher von Windows gespeichert hat. Um bereits eingerichtete Berechtigungen unwirksam werden zu lassen, widerrufen Sie bitte das gewünschte Zertifikat.

6.7 Verschlüsselte Laufwerke zentral verwalten (Zentral verwaltete Ordner)

Mit Hilfe der DriveLock Management Konsole (DMC) verwalten Sie verschlüsselte Verzeichnisse an zentraler Stelle. Sie gelangen zur Verwaltung der Verzeichnisse, in dem Sie im Navigationsbereich auf **DriveLock File Protection** und dann auf **Zentral verwaltete Ordner** klicken.

Auf der rechten Seite werden Ihnen eine Übersicht über alle in der DriveLock Datenbank gespeicherten Verzeichnisse und deren Status angezeigt.

Hier können Sie neue Verzeichnisse anlegen und Benutzerberechtigungen einmalig einrichten, Berechtigungen bestehender Verzeichnisse ändern oder ansehen (sofern Sie als Benutzer selbst die Berechtigung als Verzeichnisadministrator haben) oder Verzeichniseinträge löschen.

Wenn Sie ein neues zentral verwaltetes Verzeichnis anlegen, beachten Sie bitte folgendes:

- Es können keine bestehenden Verzeichnisse zentral verwaltet und verschlüsselt werden. Erstens ist in den meisten Fällen auf einem Server kein DFP Dienst installiert, der für eine asynchrone Verschlüsselung sorgen könnte und zweitens können während der Zeitdauer der Initialverschlüsselung auftretende Konfliktsituationen technisch nicht ausreichend genug gelöst werden (z.B. wenn erst ein Teil der Dateien bereits verschlüsselt ist oder eine größere Datei gerade verschlüsselt wird und ein anderen Benutzer von seinem Computer aus auf diese Datei zugreift).
- Die Benutzer, die beim Anlegen des Verzeichnisses für den Zugriff autorisiert werden, erhalten Administrationsrechte für dieses Verzeichnis. Administrationsrechte erlauben es, weitere Benutzer zu berechtigen bzw. Berechtigungen zu entfernen. Somit können Sie als IT-Administrator die Verwaltung der autorisierten Benutzer bereits beim Anlegen des Verzeichnisses an einen oder mehrere Benutzer der Fachabteilung abgeben.

6.7.1 Vorbereitungen im Active Directory

Um ein Netzlaufwerk (UNC-Pfad) mit DriveLock File Protection zentral verschlüsseln und verwalten zu können, müssen im Active Directory einige Vorbereitungen getroffen werden.

Die Verschlüsselung basiert auf benutzerbezogenen Zertifikaten (EFS-Zertifikaten). Diese müssen zu Beginn für jeden Benutzer erstellt werden. Hierzu bietet sich das Active Directory als zentraler Herausgeber für Zertifikate an.

Active Directory Zertifikatsdienste: Zertifikate mit Gruppenrichtlinien verteilen

Eine Active Directory-integrierte CA bietet die Möglichkeit, Zertifikate automatisch über Gruppenrichtlinien an Benutzer oder Computer zu verteilen. Im folgenden wird Auto-Enrollment durch eine duplizierte Zertifikat-Vorlage **Basis-EFS** konfiguriert. Diese dient der Verschlüsselung von Ordnerinhalten.

Folgende Schritte müssen dabei durchgeführt werden:

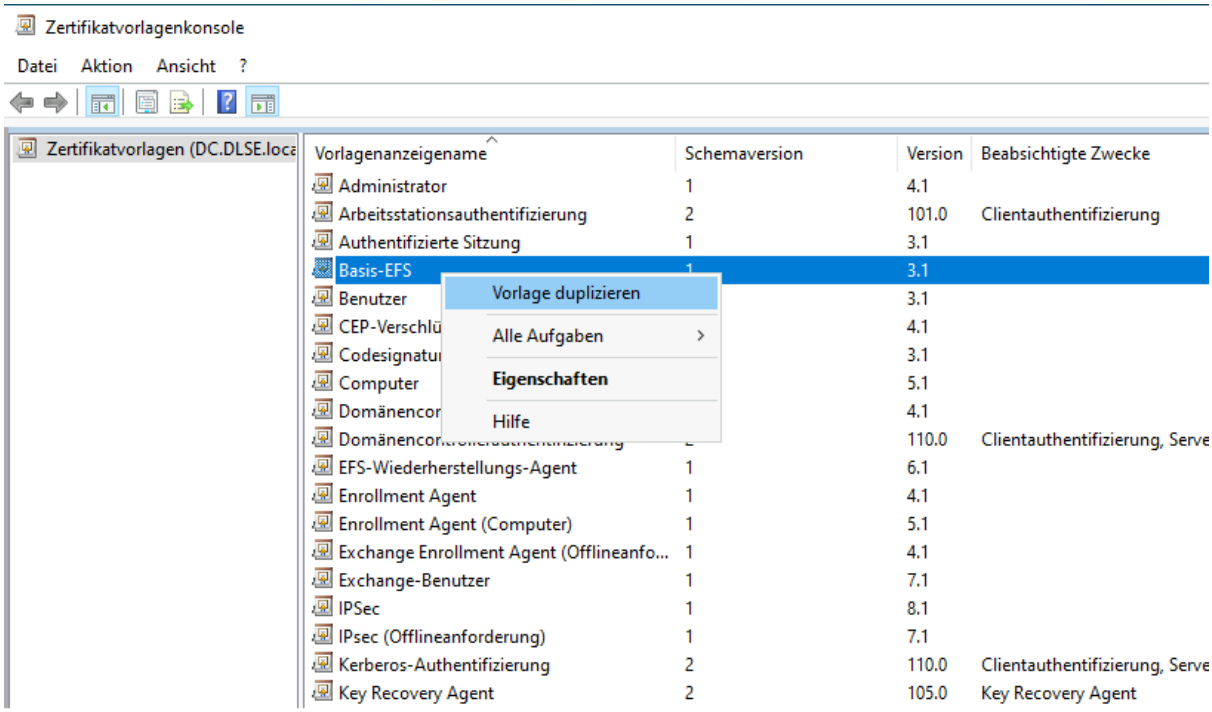
1. Duplizieren der Zertifikatsvorlage
2. Ausstellen der Vorlage
3. Erstellen einer Gruppenrichtlinie
4. Automatische Registrierung und Aktivieren der Richtlinie (Certificate Credential Roaming)
5. Testen der automatischen Registrierung

Dann erst kann die Konfiguration in der DriveLock Management Konsole (DMC) erfolgen. Einen konkreten Anwendungsfall finden Sie hier.

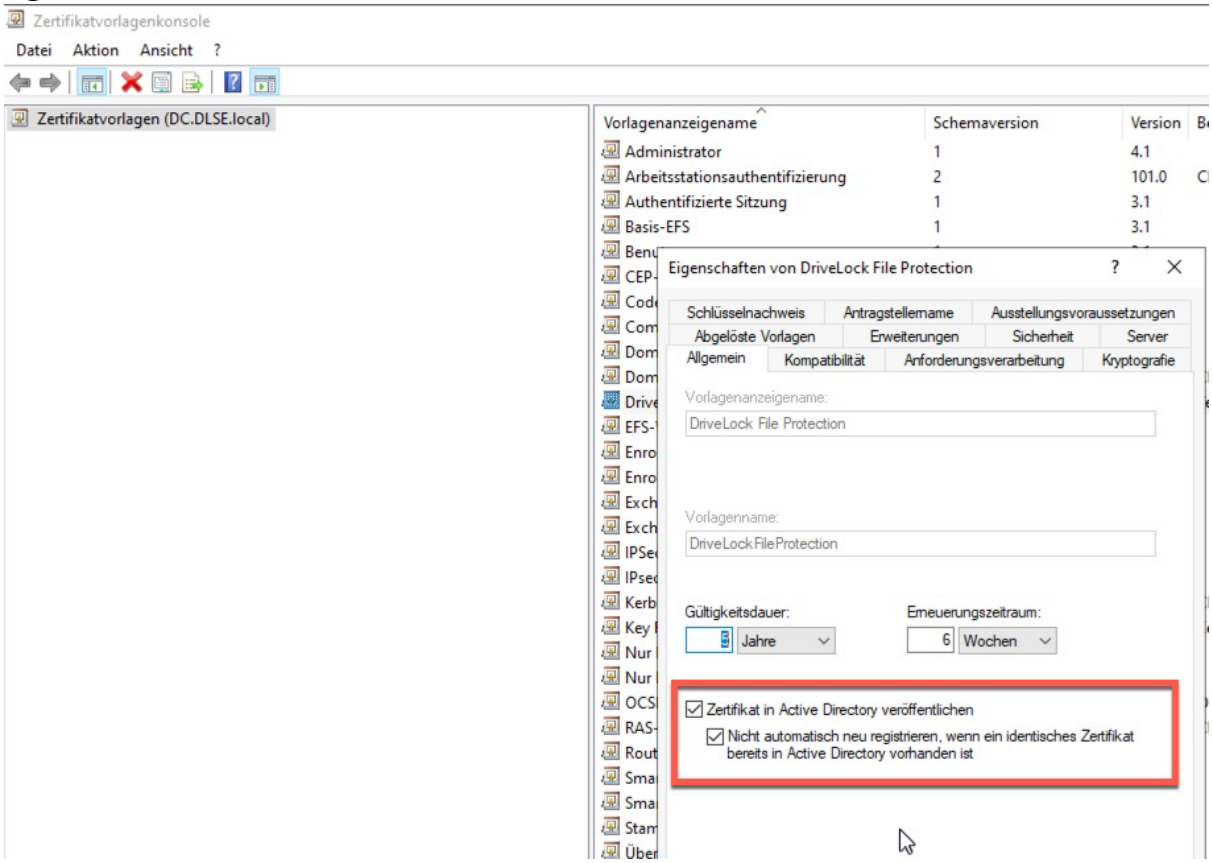
6.7.1.1 Duplizieren der Zertifikatsvorlage

Zum Duplizieren der Zertifikatsvorlage gehen Sie folgendermaßen vor:

1. Öffnen Sie am CA-Server die Zertifikatvorlagenkonsole **certtmpl.msc** und klicken die Vorlage **Basis-EFS** mit der rechten Maustaste an.
2. Wählen Sie **Vorlage duplizieren**.

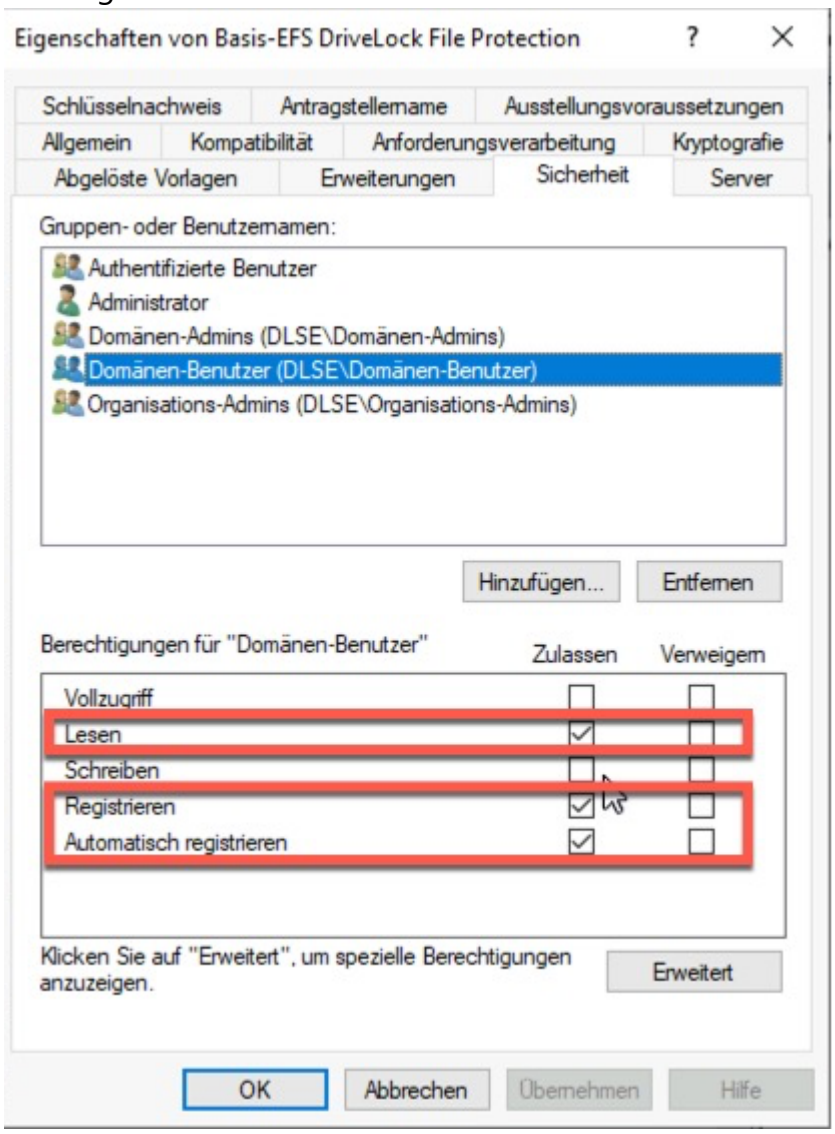


3. Geben Sie auf dem Reiter **Allgemein** einen geeigneten **Namen** und die **Gültigkeitsdauer** an.

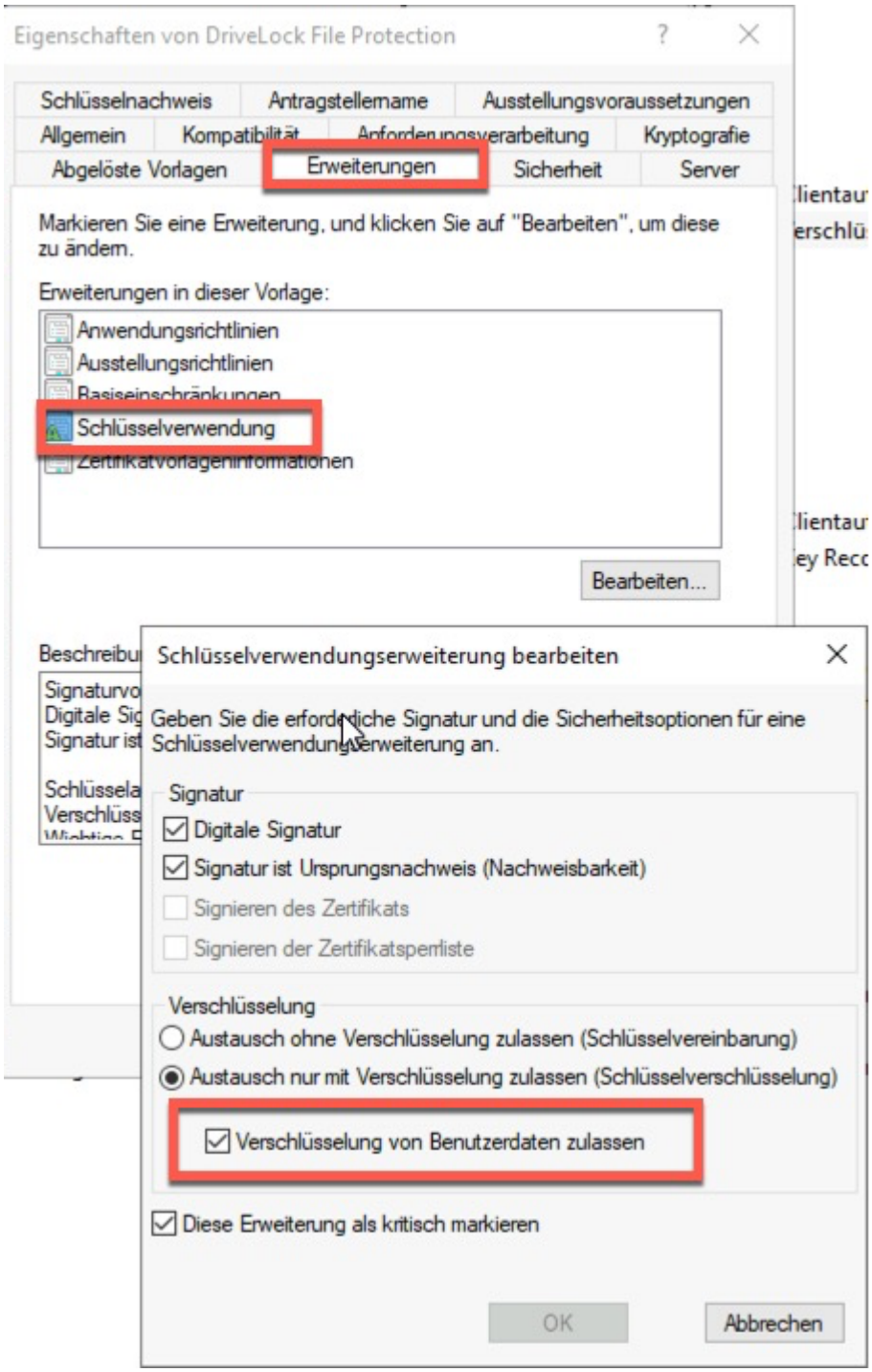


4. Bestätigen Sie mit **Übernehmen**.

5. Öffnen Sie jetzt in den Eigenschaften des Basis-EFS DriveLock File Protection den Reiter **Sicherheit**.
6. Um Auto-Enrollment zu konfigurieren, weisen Sie dem Benutzer die Rechte **Lesen**, **Registrieren** und **Automatisch registrieren** zu und bestätigen Sie diese Einstellungen.



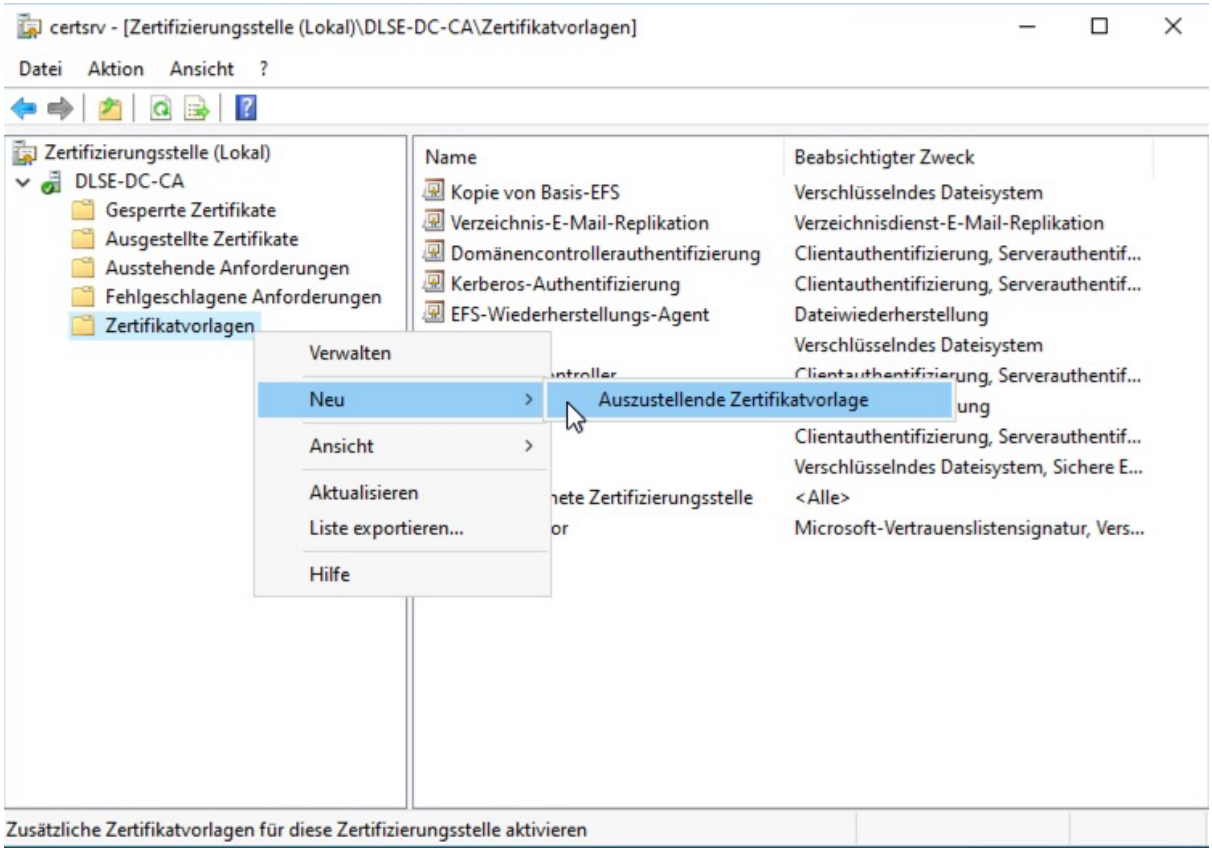
7. Setzen Sie auf dem Reiter **Erweiterungen** in der **Schlüsselverwendung** ein Häkchen bei der Option **Verschlüsselung von Benutzerdaten zulassen** und bestätigen Sie mit **OK**.



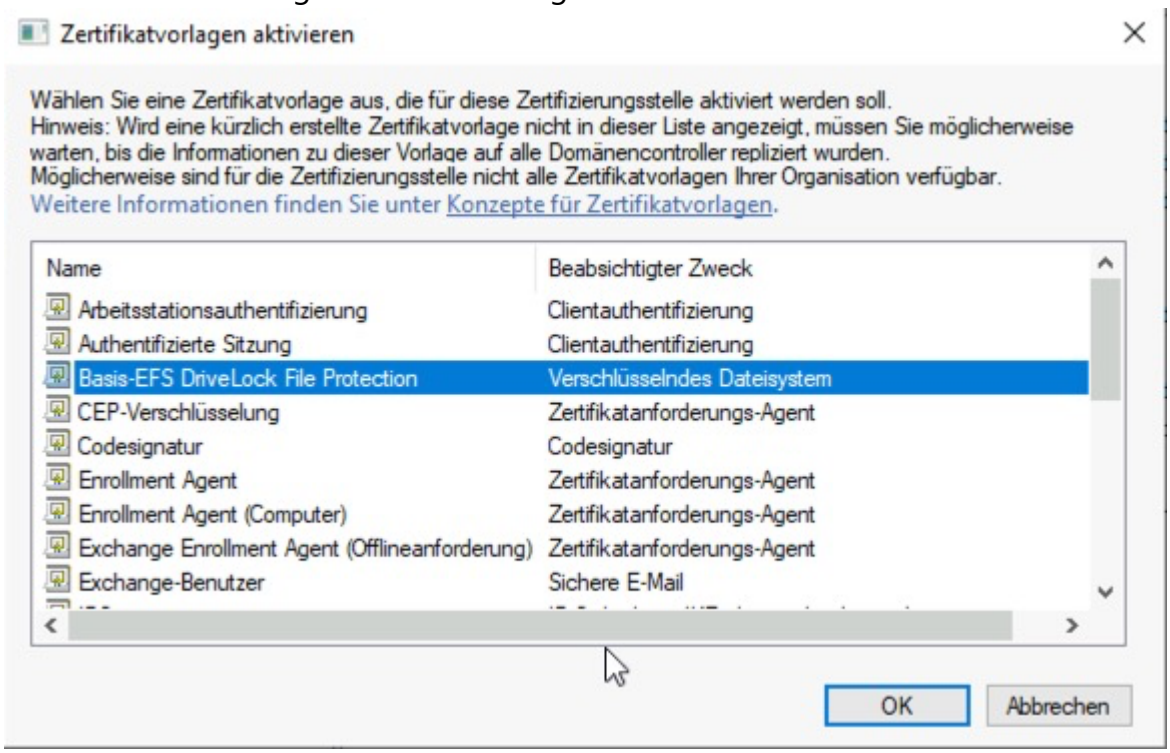
6.7.1.2 Ausstellen der Vorlage

Zum Ausstellen der Zertifikatsvorlage gehen Sie folgendermaßen vor:

1. Wählen Sie am CA-Server **certsrv.msc** im Kontextmenü **Neu** die Option **Auszustellende Zertifikatvorlage**.



2. Wählen Sie die Vorlage aus und bestätigen diese mit **OK**.

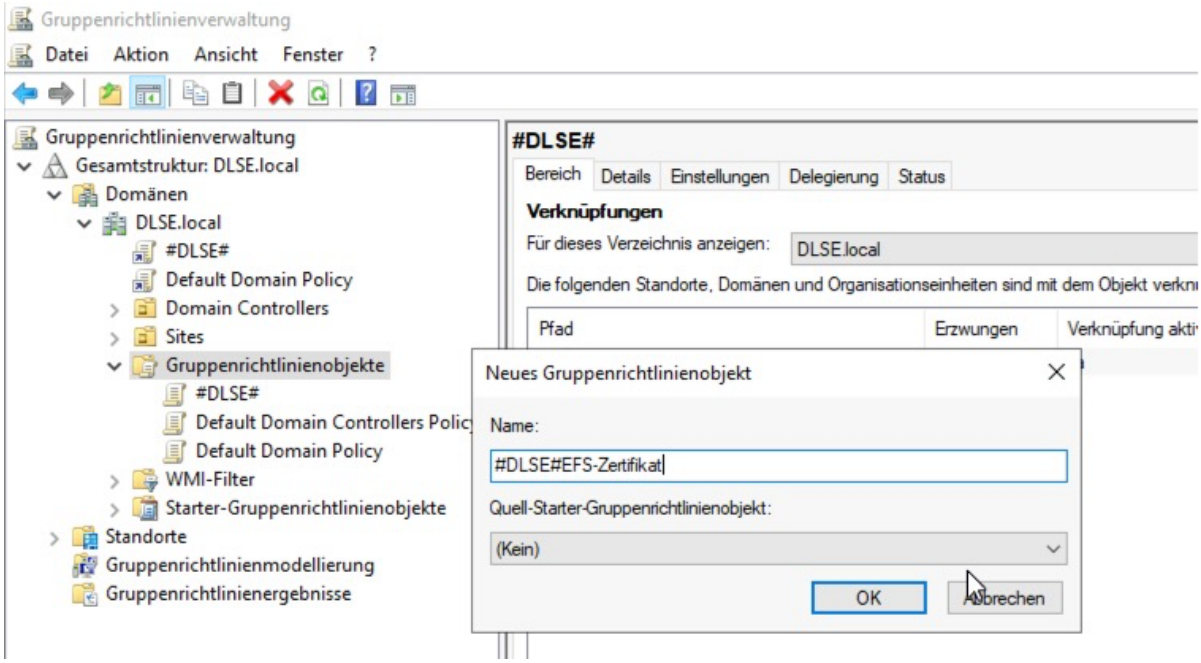


3. Prüfen Sie die Vorlage. Die Vorlage ist nun konfiguriert und ausgestellt.
4. Als nächstes richten Sie eine Gruppenrichtlinie ein.

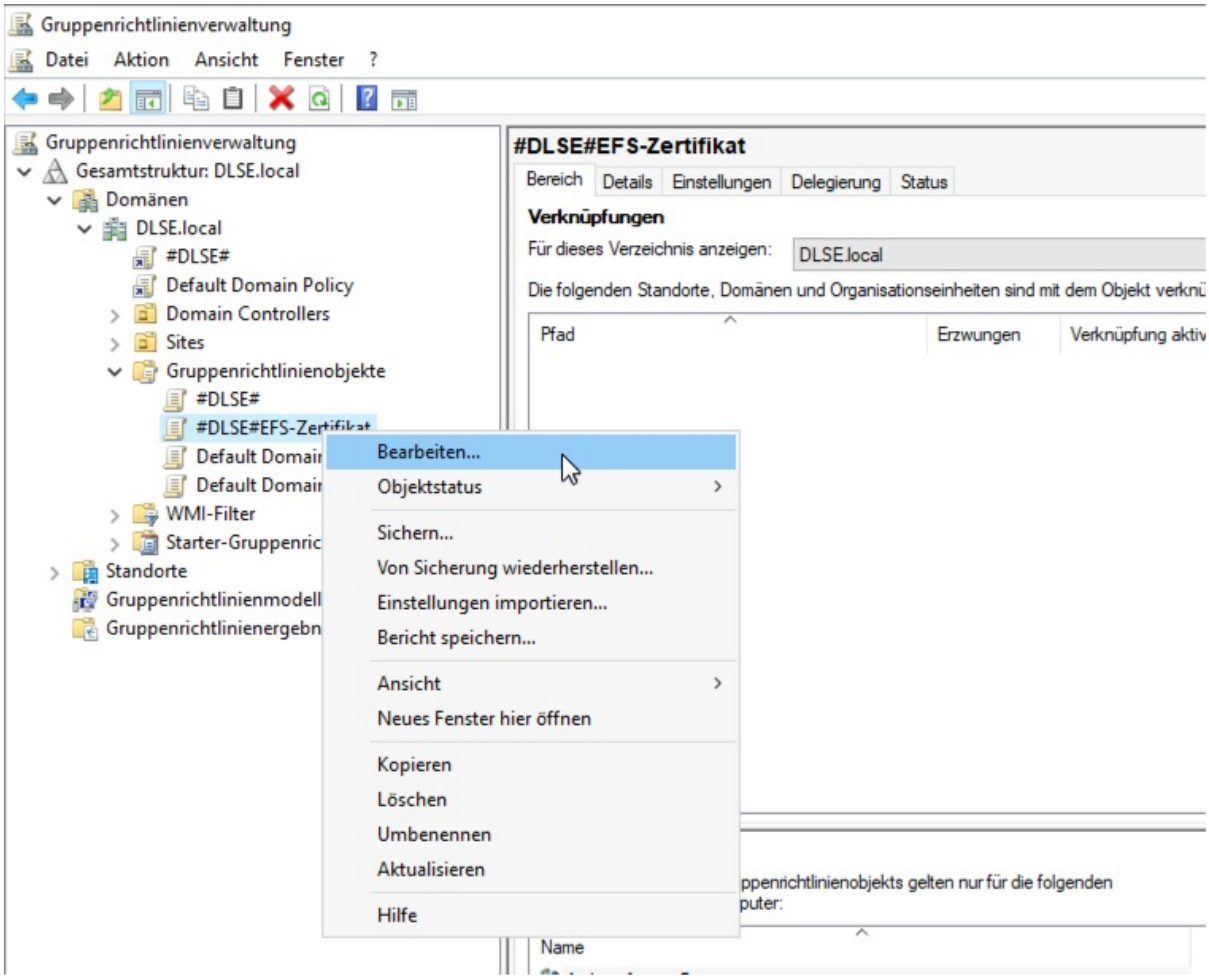
6.7.1.3 Erstellen einer Gruppenrichtlinie

Zum Erstellen einer Gruppenrichtlinie gehen Sie folgendermaßen vor:

1. Öffnen Sie **gpmc.msc** auf einem Domain-Controller, wählen Sie die **Gruppenrichtlinienobjekte** und dann **Neu** .



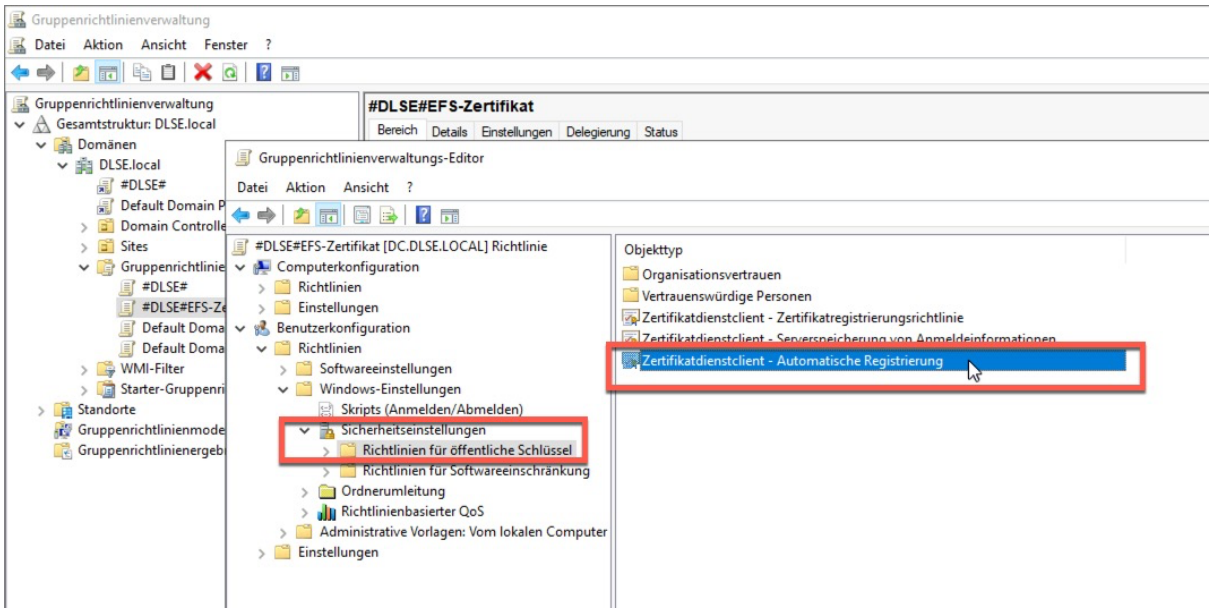
2. Öffnen Sie das Kontextmenü des GPO und wählen Bearbeiten... .



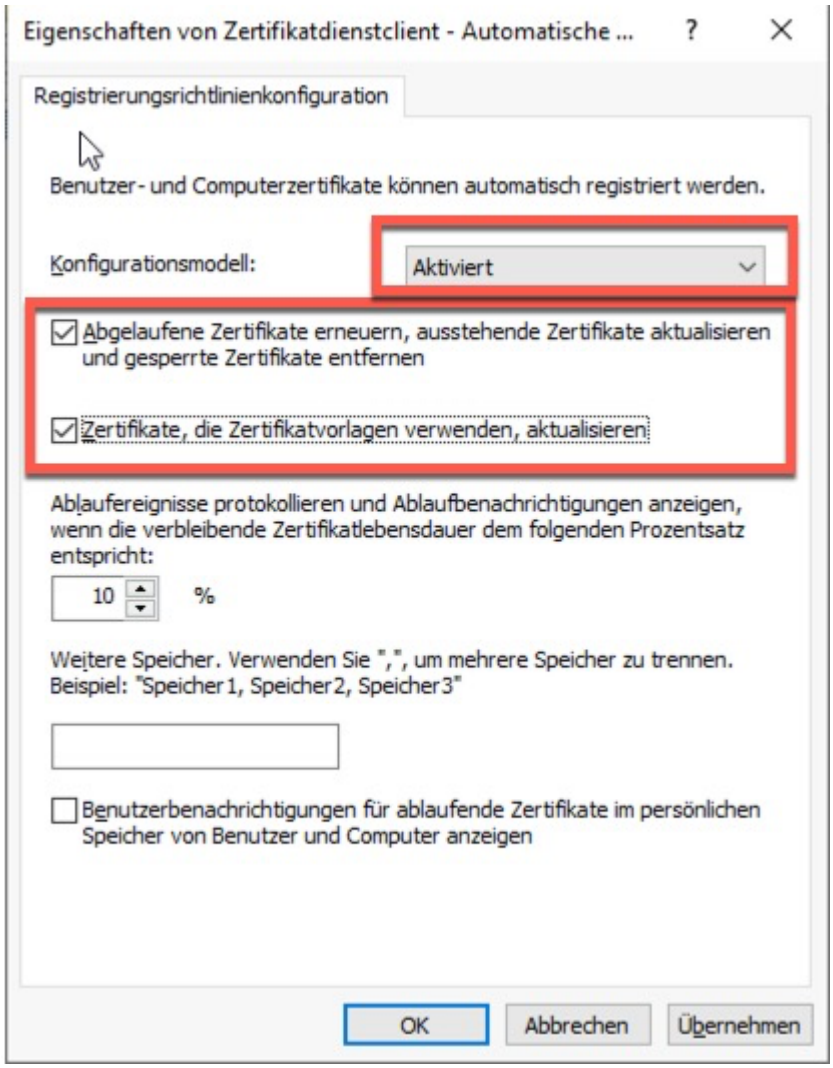
6.7.1.4 Automatische Registrierung

Zur automatischen Registrierung und Aktivierung der GPO gehen Sie folgendermaßen vor:

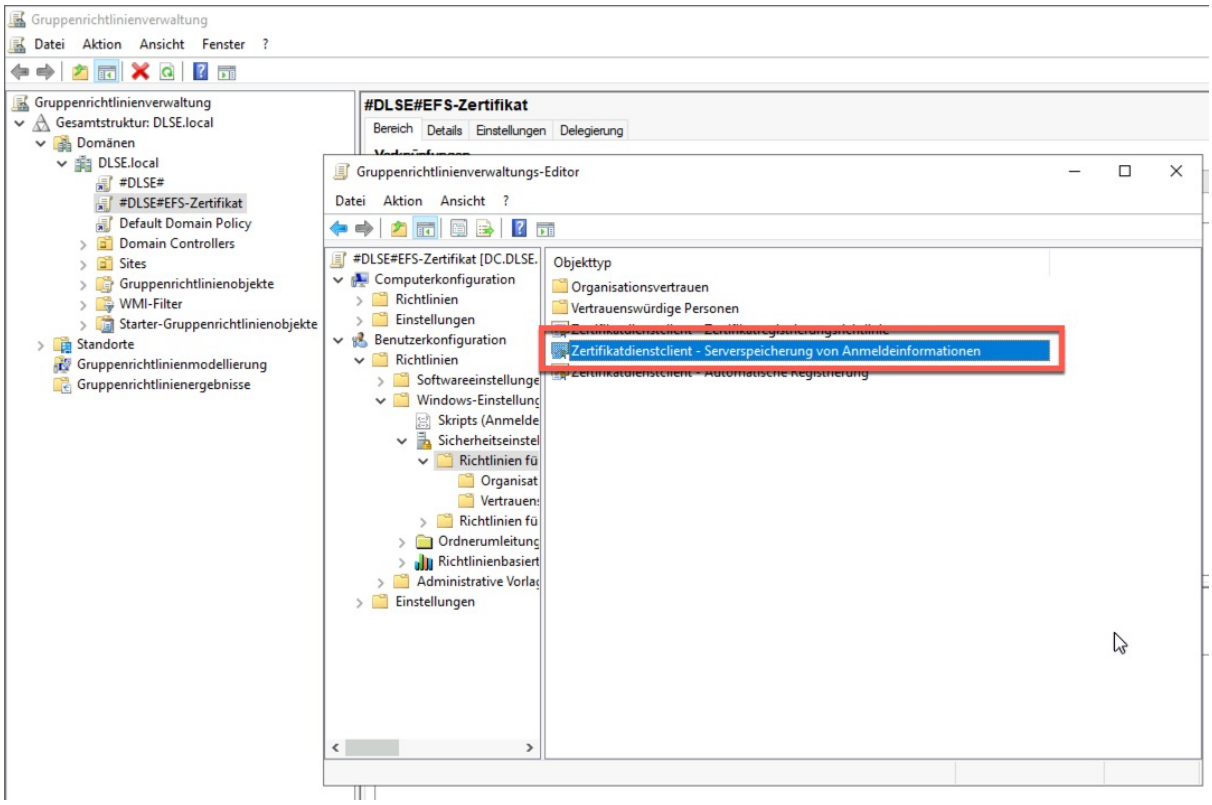
1. Öffnen Sie unter **Benutzerkonfiguration** den Ordner **Richtlinien**, dann **Windows-Einstellungen**und **Sicherheitseinstellungen**.



2. Unter den Richtlinien für öffentliche Schlüssel finden Sie **Zertifikatsdienstclient – Automatische Registrierung**. Öffnen Sie die Eigenschafen dieses Objekttyps und wählen Sie hier folgende Optionen aus:



3. Damit das Benutzerzertifikat auf alle Computer im Netzwerk mitwandern kann ("Certificate Credential Roaming"), muss die **Serverspeicherung von Anmeldeinformationen** aktiviert werden.

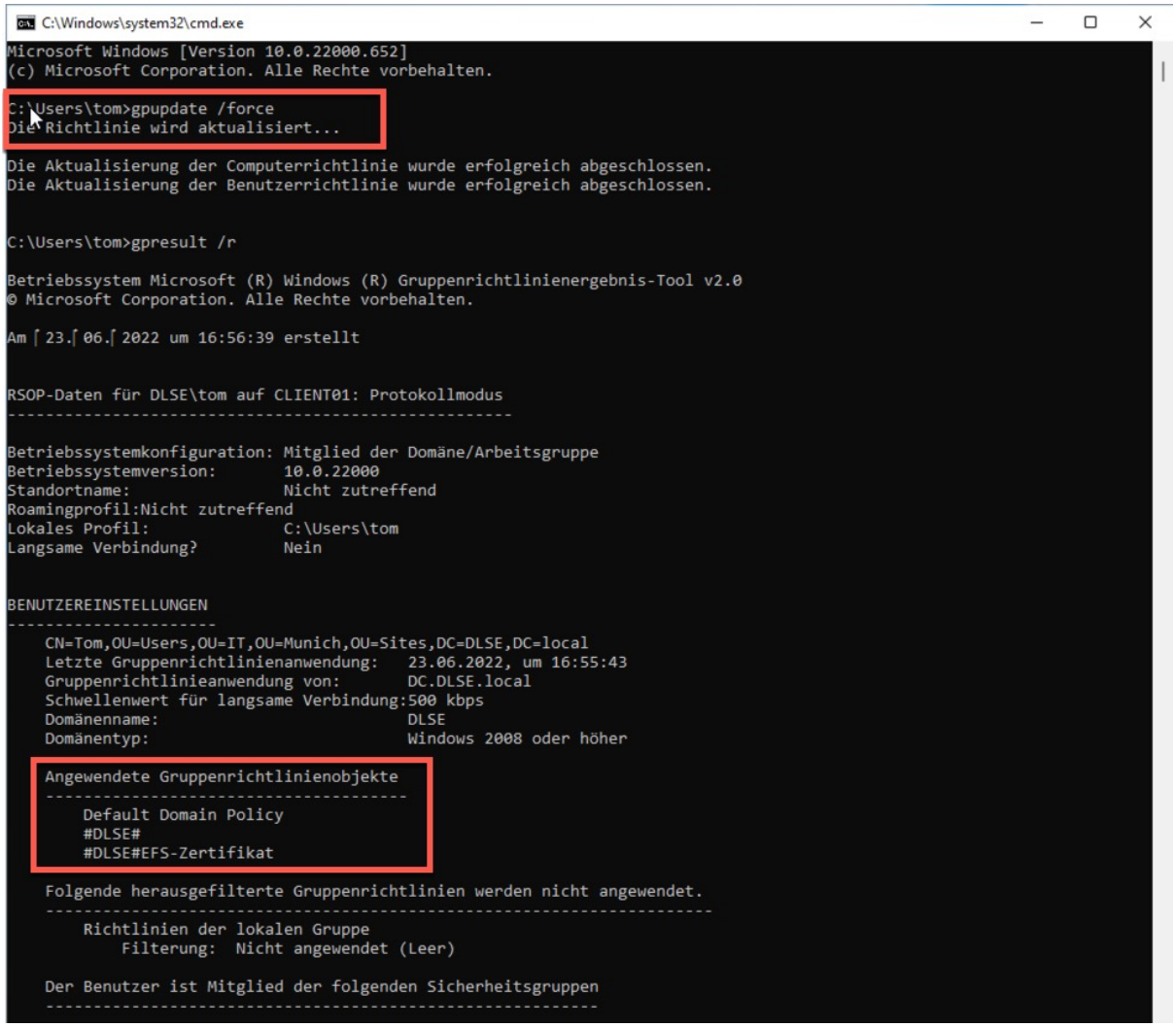


4. Öffnen Sie den entsprechenden Objekttyp und wählen Sie auf dem Reiter **Allgemein** die Option **Aktiviert**.
5. Bestätigen Sie Ihre Einstellungen mit **OK** und schließen Sie den Gruppenrichtlinien-Editor.
6. Verknüpfen Sie anschließend das GPO noch mit der Domäne, der OU oder einem Standort. Sie können beispielsweise das GPO mit der OU "Mitarbeiter" verknüpfen, das Objekt über diese OU ziehen und dann die Maustaste loslassen.

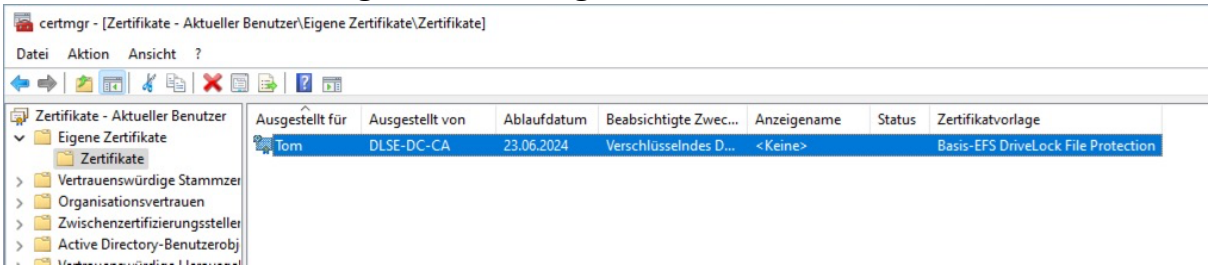
6.7.1.5 Testen der automatische Registrierung

Zum Testen gehen Sie folgendermaßen vor:

1. Starten Sie einen Windows 11 Client der Active Directory Domäne und melden sich mit einem Benutzer an.
2. Damit das neu gesetzte GPO definitiv zieht, können Sie einen Group Policy Refresh in einer DOS-Box ausführen.
3. `gpupdate /force`: Hiermit überprüfen Sie, dass das GPO angewandt wurde
4. `gpresult /r`



5. Das Zertifikat ist in **certmgr.msc** unter **Eigene Zertifikate** – **Zertifikate** zu finden.



6.7.2 Neues verschlüsseltes Laufwerk anlegen

Hinweis: Sie benötigen Schreibrechte für das Verzeichnis bzw. das Netzlaufwerk, in dem Sie das neue verschlüsselte Verzeichnis anlegen möchten.

Um ein neues verschlüsseltes Verzeichnis anzulegen, führen Sie folgende Schritte durch:

1. Rechtsklicken Sie auf **Zentral verwaltete Ordner** im Navigationsbereich oder auf eine leere Stelle in der Detailansicht rechts

2. Wählen Sie **Neu** und **Zentral verwalteter Ordner...** .
3. Optional: Die Einstellungen **Erzeugen für Mandant** und **Primärer Server** müssen nur angepasst werden, wenn in Ihrer Umgebung mehr als ein DES verfügbar ist und ein anderer DES als der zentrale Service verwendet werden soll, oder Sie mehr als einen Mandanten eingerichtet haben und nicht der Standard-Mandant root verwendet werden muss. In den meisten Fällen dürfte keine Änderung dieser Vorgaben notwendig sein.
4. Geben Sie in das Textfeld **Pfad des neuen zentral verwalteten Ordners** den UNC-Pfad für das neue Verzeichnis an.

Alternative:

1. Klicken Sie auf die Schaltfläche **...** und wählen Sie über den Auswahldialog das gewünschte Verzeichnis aus. Klicken Sie auf **Neues Verzeichnis**, um im zuvor ausgewählten Ordner ein neues Verzeichnis anzulegen und wählen Sie dieses aus.
2. Vergewissern Sie sich, dass der nun angezeigte UNC-Pfad korrekt ist.
3. Um einen bestimmten Benutzer zu suchen, geben Sie einen Suchtext in das obere Suchfeld ein.
4. Wählen Sie nun eine oder mehrere angezeigte Benutzer aus. Diese erhalten nach der Einrichtung administrative Berechtigungen für dieses Verzeichnis.
5. Klicken Sie auf **Weiter**. Der neue Ordner wird nun angelegt und die Berechtigungen eingetragen. Anschließend erhalten Sie eine Rückmeldung, ob dieser Vorgang erfolgreich abgeschlossen werden konnte.
6. Klicken Sie auf **Fertig stellen**. Der Ordner ist nun verschlüsselt.

Einen konkreten Anwendungsfall finden Sie hier.

6.7.3 Zugriffsberechtigungen ändern

Die Zugriffsberechtigungen für einen verschlüsselten Ordner können entweder durch die DriveLock Benutzeroberfläche, über das Kontextmenü im Windows Explorer oder über die DriveLock Management Konsole geändert werden. Für die Änderung benötigt der durchführende Benutzer administrative Berechtigungen für dieses Verzeichnis.

Um als Administrator über den Windows Explorer die Zugriffsberechtigungen zu ändern, rechts-klicken Sie auf das Verzeichnis und wählen Sie Eigenschaften und Benutzer des verschlüsselten Ordners.

Um als Administrator über die DriveLock Management Konsole die Zugriffsberechtigungen für ein bestehendes zentral verwaltetes Verzeichnis zu ändern, gehen Sie folgendermaßen vor:

1. Klicken Sie auf Zentral verwaltete Ordner im Navigationsbereich.
2. Rechtsklicken Sie auf das gewünschte Verzeichnis in der Detailansicht und wählen Sie Ordner verwalten.

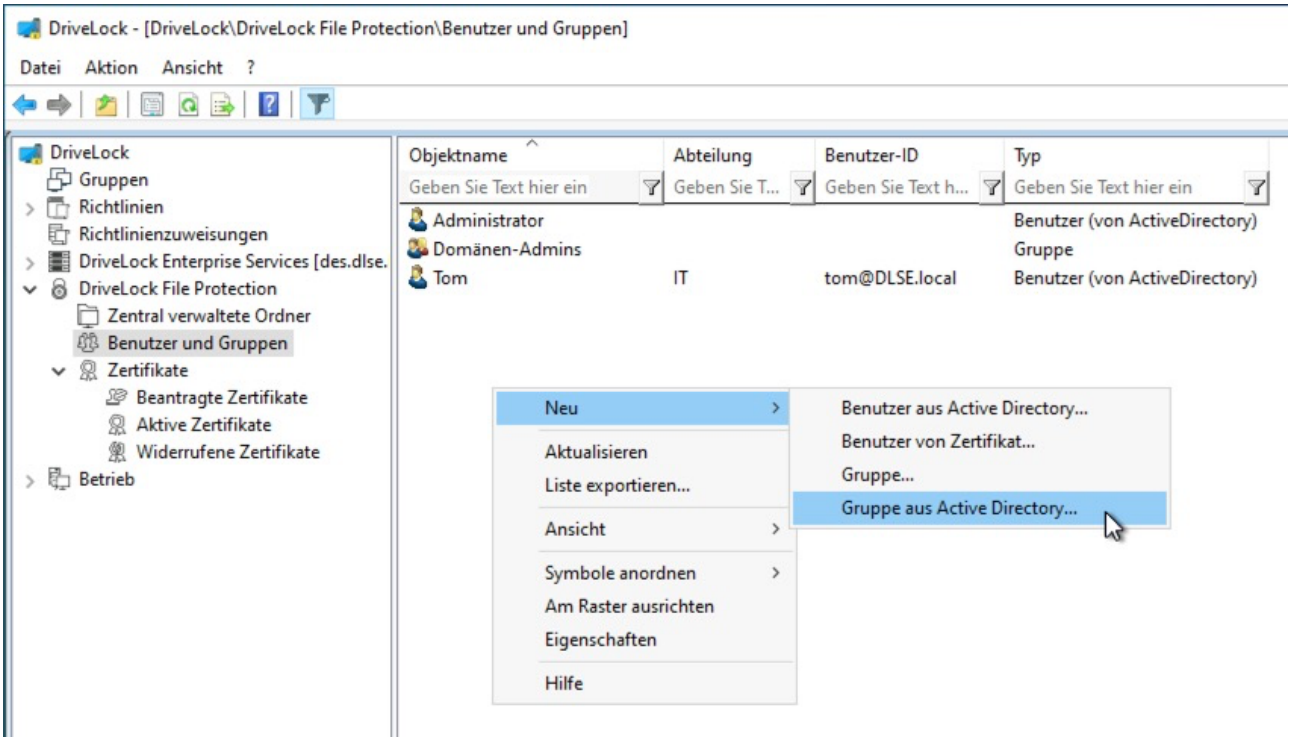
Alternative:

1. Doppelklicken Sie auf das gewünschte Verzeichnis, wählen Sie den Reiter **Benutzer** und klicken Sie auf **Verwalten**.
2. Sofern bei den Informationen <Anmelden um Daten zu sehen> angezeigt wird, müssen Sie sich zunächst noch Authentifizieren. Klicken Sie dazu auf **Anmelden** und wählen Sie das Zertifikat, welches für den Zugriff benötigt wird, aus.
3. Wählen Sie den Reiter **Benutzer**.
4. Um einen Benutzer den Zugriff zu entziehen, wählen Sie den gewünschten Benutzer aus und klicken Sie auf **Entfernen**.
5. Um einen neuen Benutzer zu berechtigen, klicken Sie auf **Hinzufügen**.

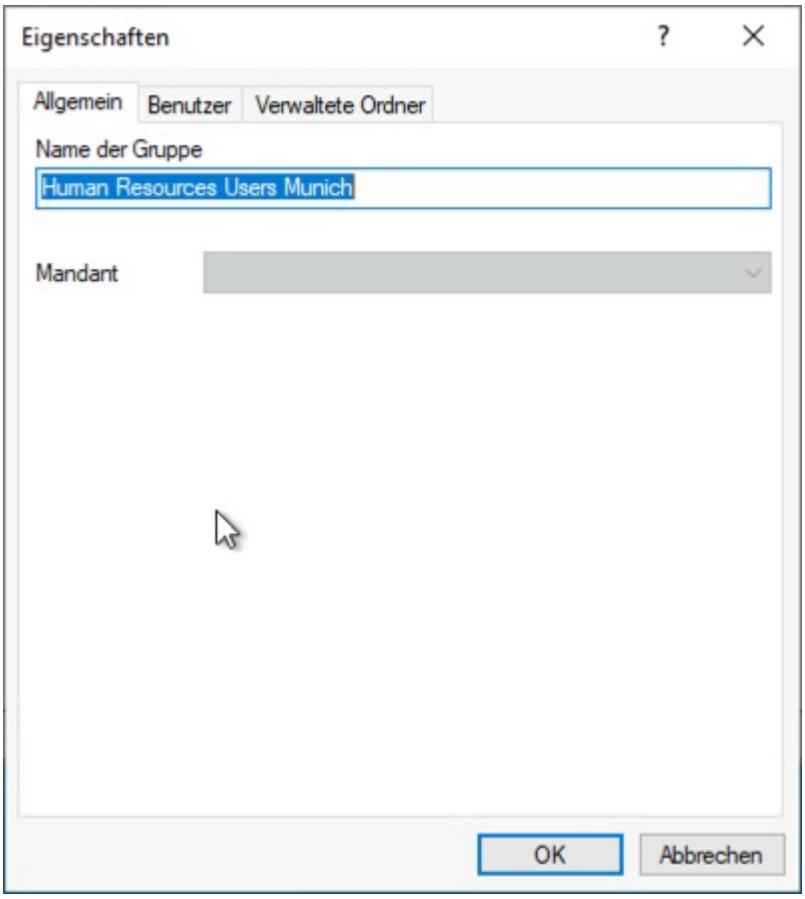
6.8 Anwendungsfall: Zugriff auf verschlüsselte Ordner

Damit Benutzer und Gruppen Zugriff auf verschlüsselte Ressourcen erhalten können, müssen Sie diese Gruppen und Benutzer aus dem Active Directory definieren.

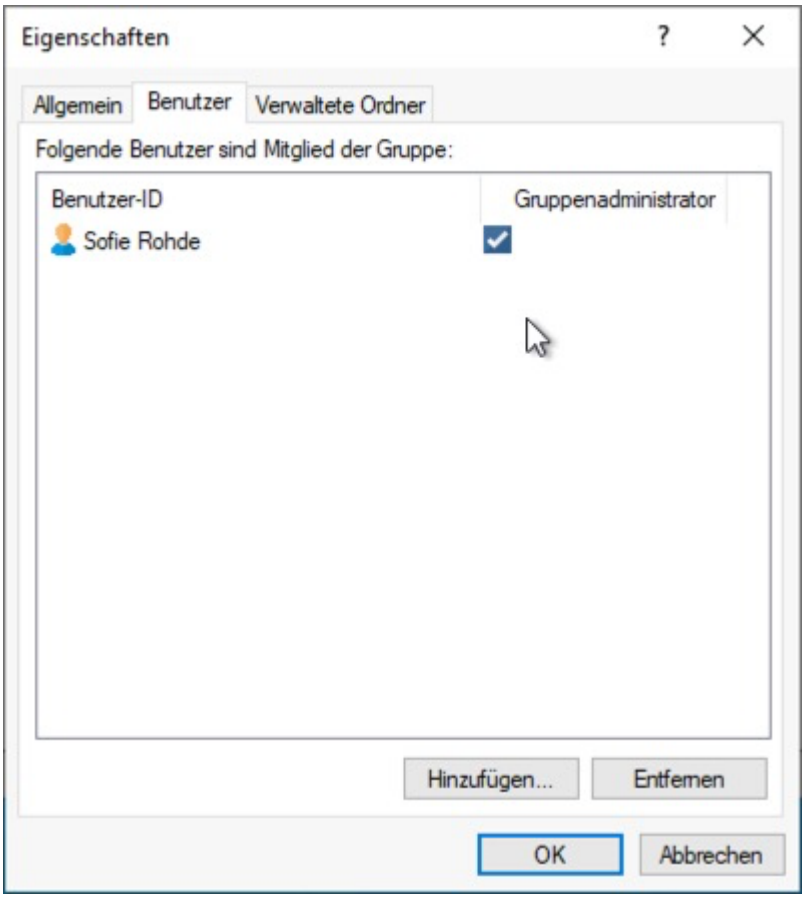
Gehen Sie hierzu im Untermenü **Benutzer und Gruppen** auf **Neu** und wählen Sie einen Benutzer oder eine Gruppe aus dem Active Directory aus.



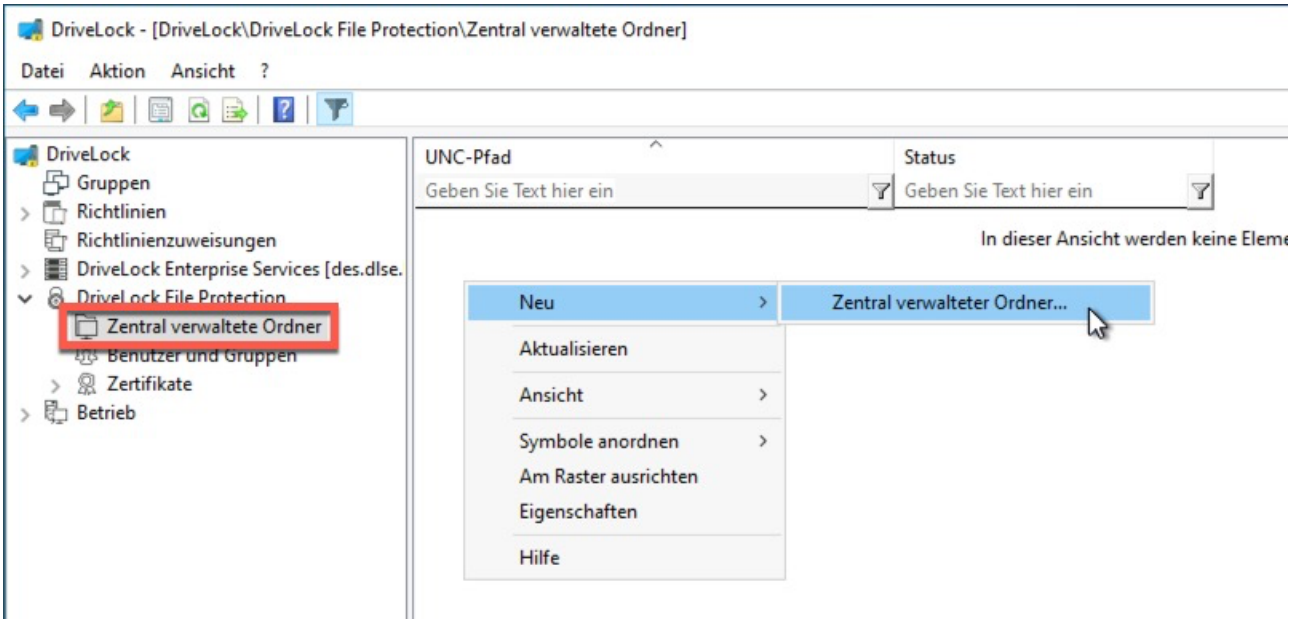
In diesem Beispiel wurde die Gruppe „Human Resources Users Munich“ gewählt.



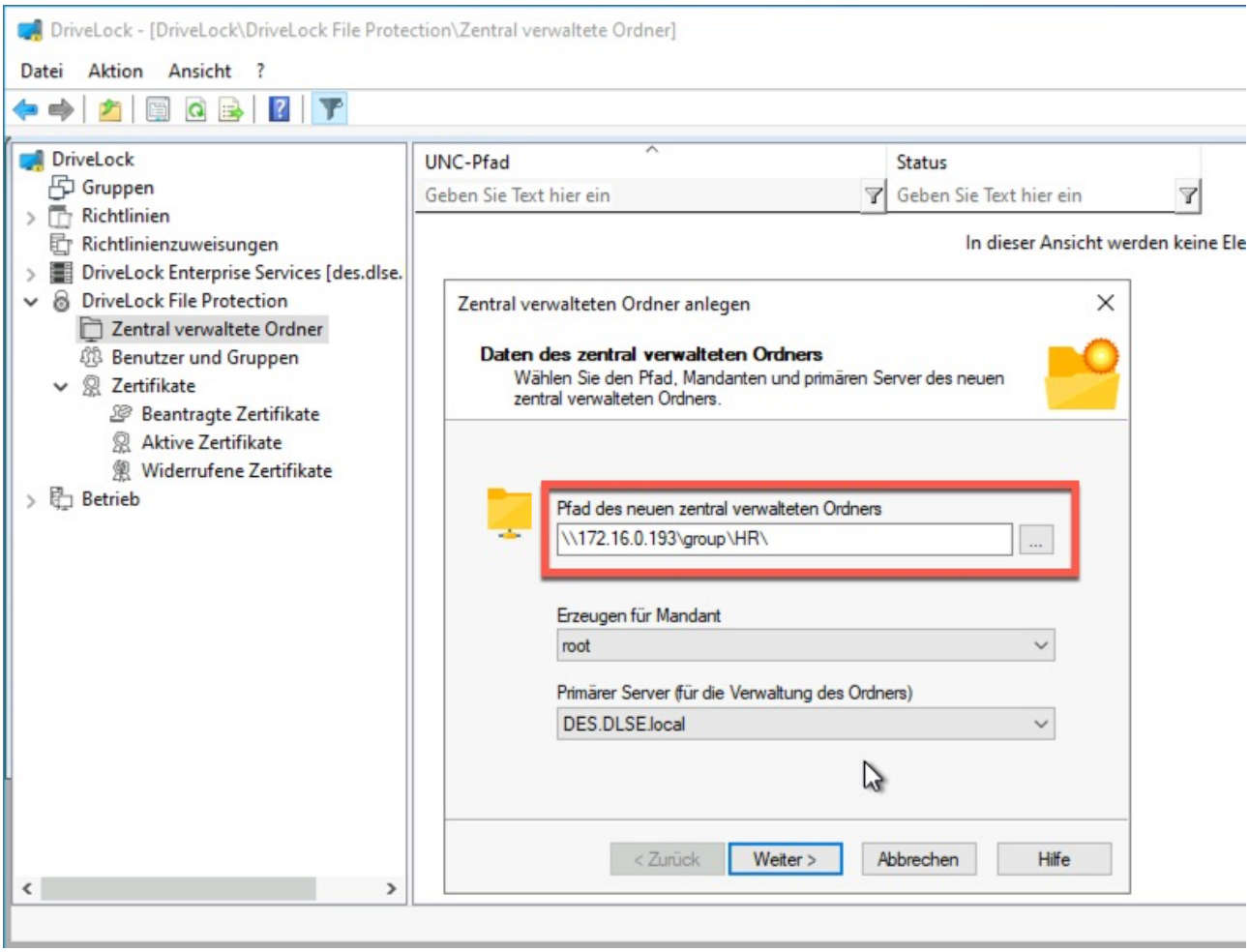
Bei Gruppen müssen Sie einen Gruppenadministrator wählen. Dieser wird auf dem Reiter **Benutzer** konfiguriert.



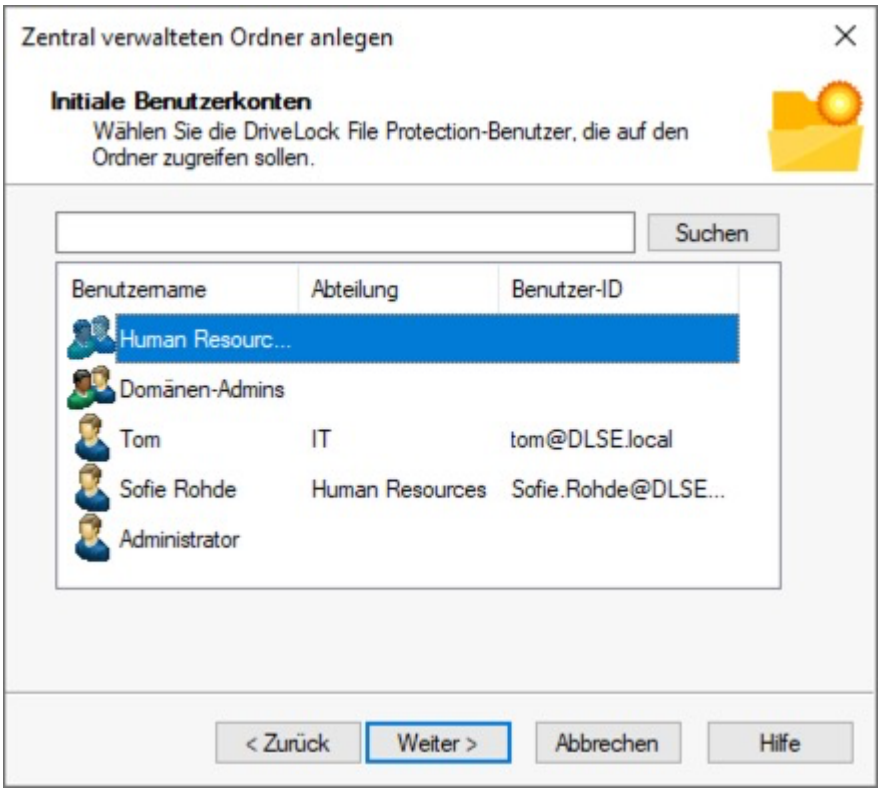
Wählen Sie nun den Unterknoten **Zentral verwaltete Ordner** und konfigurieren Sie einen neuen zentral verwalteten Ordner.

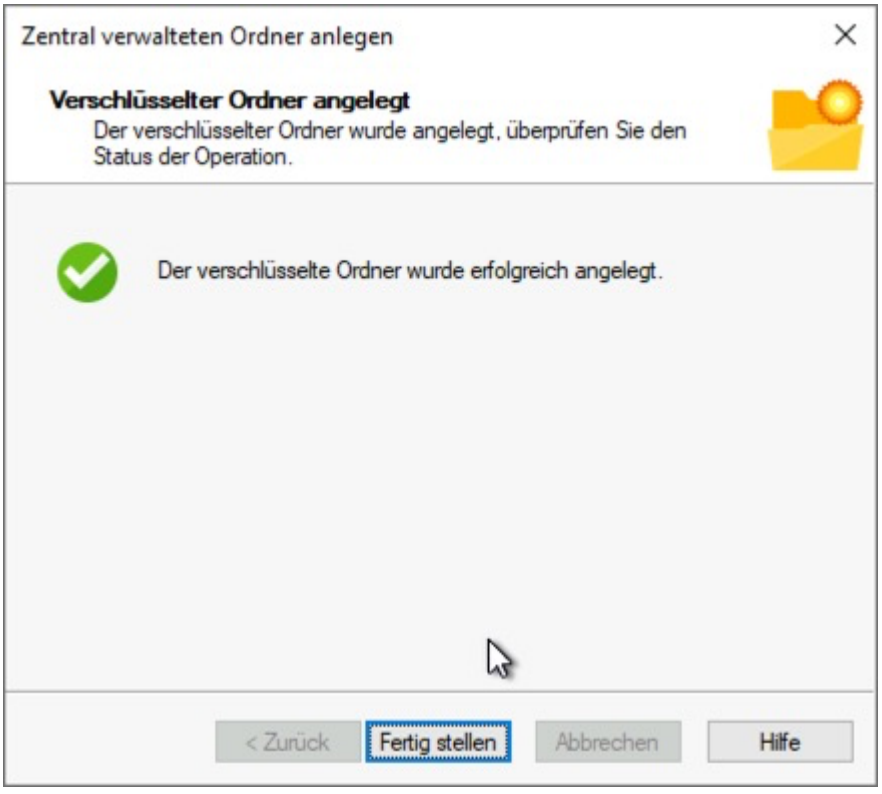


Geben Sie hier den UNC Pfad zum Netzlaufwerk bzw. dem veröffentlichten Ordner an, welcher mit DriveLock File Protection verschlüsselt werden soll.

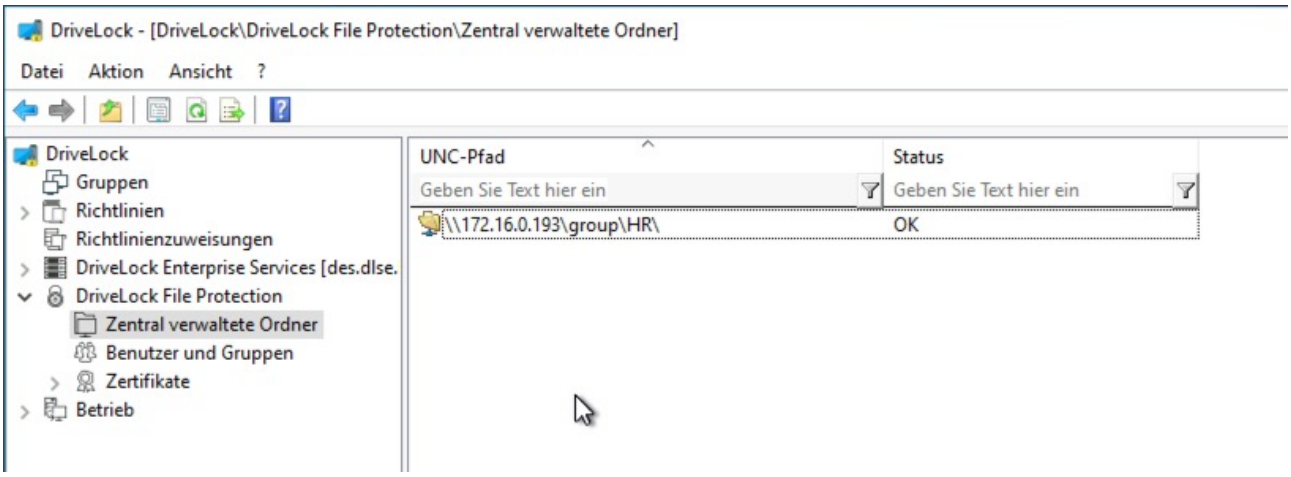


Wählen Sie die im vorherigen Schritt hinzugefügte Gruppe oder Benutzer aus.

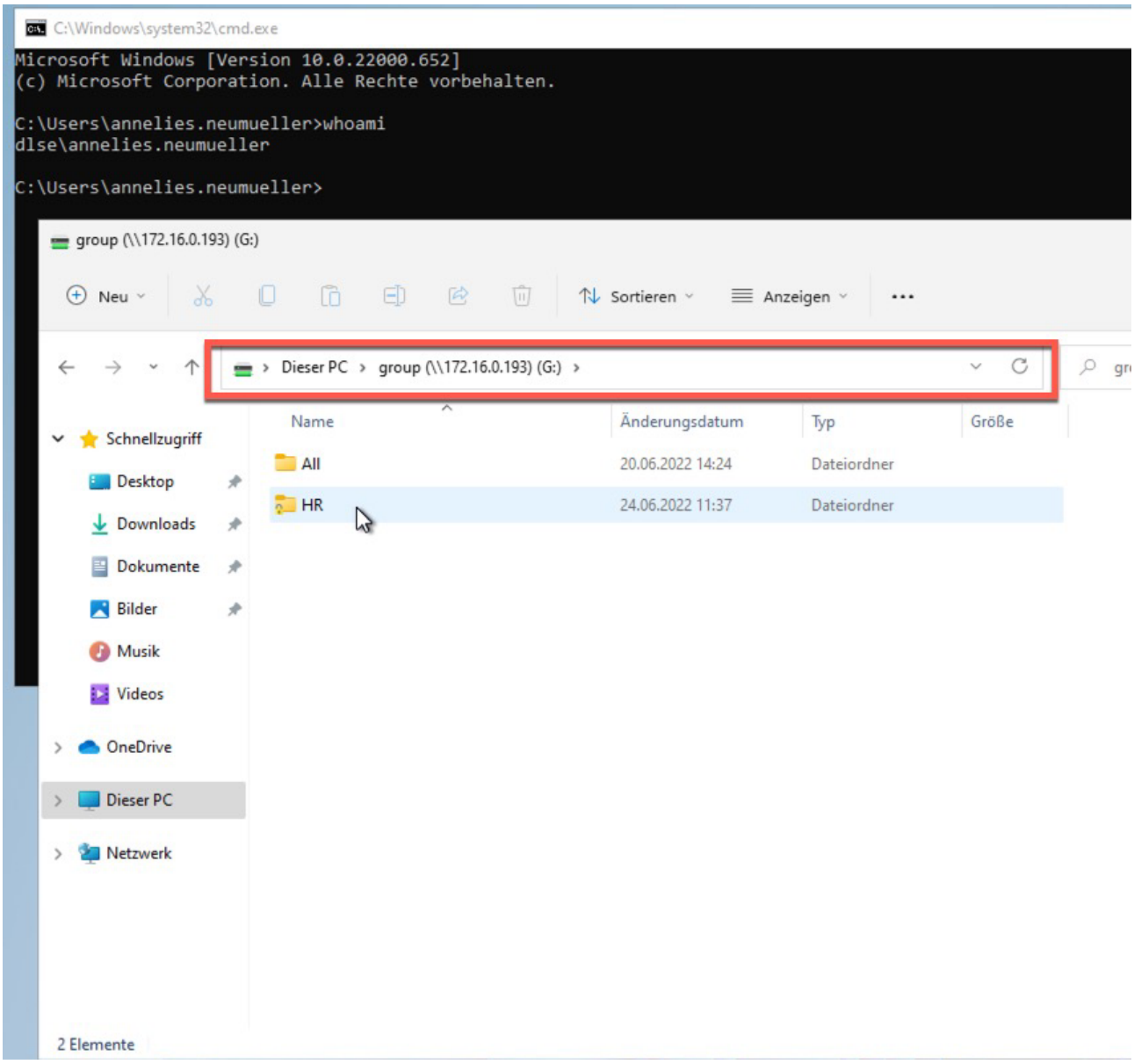




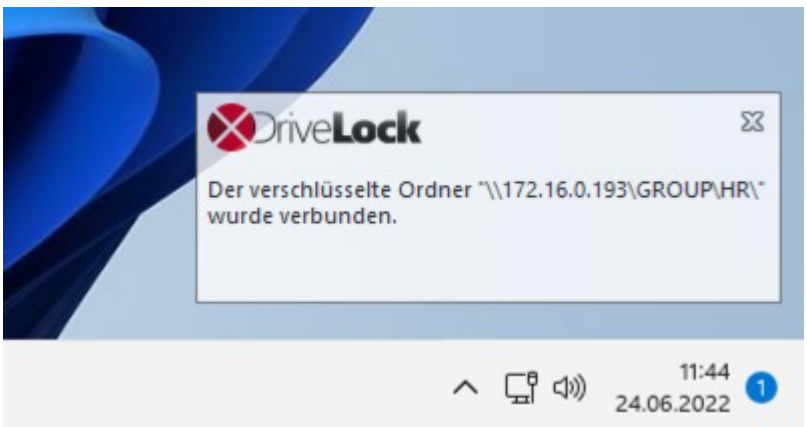
Klicken Sie auf „Fertig stellen“. Der Ordner ist nun verschlüsselt.



Sie können sich nun an einem Computer, der Mitglied der Domäne ist, anmelden. In diesem Beispiel melden wir „Annelies Neumüller“ an. Annelies ist Mitglied der Gruppe „Human Resource Users Munich“.



Sobald der Benutzer auf den Ordner im Netzwerk klickt, wird dieser vom DriveLock Agent entschlüsselt und eingebunden. Eine entsprechende Mitteilung erscheint hierzu im Mitteilungsbereich.



6.9 Wiederherstellung verschlüsselter Verzeichnisse

Sie benötigen die Wiederherstellung verschlüsselter Verzeichnisse, wenn kein Benutzer mehr auf ein verschlüsseltes Verzeichnis zugreifen und die Daten entschlüsseln kann. Dies kann entweder durch den Verlust der entsprechenden Benutzerzertifikate oder das Vergessen eines Passwortes geschehen.

Um den Zugriff auf verschlüsselte Laufwerke wiederherzustellen, nachdem ein Passwort vergessen oder ein Zertifikat verloren ging, wird eine sogenannte Offline-Wiederherstellung mit Hilfe eines Challenge-Response Verfahrens durchgeführt. Dabei sind der Benutzer und der Administrator (oder Support-Mitarbeiter(-in)) involviert.

Das Challenge-Response Verfahren beruht auf der Überprüfung eines Anforderungscodes (Challenge) und der Generierung eines Antwortcodes (Response), welches wiederum überprüft wird. Wenn beide Codes korrekt sind, kann der Zugriff wiederhergestellt bzw. erneuert werden (z.B. durch das Vergeben eines neuen Passwortes). Der Anforderungscode wird vom Benutzer mit Hilfe eines Assistenten generiert, an den Administrator übermittelt und durch diesen auf Gültigkeit überprüft. Ist der Code in Ordnung, wird vom System ein Antwortcode generiert, durch den Administrator an den Benutzer übermittelt und durch diesen mit Hilfe des Assistenten wieder überprüft.

Die für die Wiederherstellung durch den Benutzer durchzuführenden Schritte werden im DriveLock Benutzerhandbuch beschrieben.

Die Schritte für die Wiederherstellung durch den Administrator (oder Support-Mitarbeiter(-in)) sind identisch zur Wiederherstellung verschlüsselter Laufwerke.

6.10 File Protection im DOC

Auswertungen, Berichte und Statistiken lassen sich mit Hilfe des DriveLock Operations Center (DOC) durchführen. Außerdem lässt sich die Wiederherstellung verschlüsselter Ordner über die Ansicht **File Protection Wiederherstellung** im DOC durchführen.

7 DriveLock Disk Protection

Disk Protection ist eine in DriveLock integrierte Sicherheits- und Daten-verschlüsselungslösung für Festplatten. Sie ist auf folgendem Betriebssystem einsetzbar:

- UEFI BIOS: Windows 10 (nur 64-bit) oder höher

DriveLock Disk Protection stellt die nachfolgenden Funktionen zur Verfügung:

- Festplattenverschlüsselung
- Pre-Boot-Authentifizierung (PBA)
- Single Sign-On oder manuelle Windows Authentifizierung
- Notfall-Wiederherstellung von Pre-Boot Benutzern und Token Anmeldungen
- Notfall-Wiederherstellungs- und Administrationstools

7.1 Einstellungen in Richtlinien

7.1.1 Verschlüsselungszertifikate

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

Folgende Zertifikate müssen erstellt werden:

- **Hauptzertifikat (MSC = Master Security Certificate):**

  Die Dateien DLFDEMaster.cer und DLFDEMaster.pfx ergeben ein öffentliches/privates Schlüsselpaar.
  DLFDEMaster.pfx wird dazu benutzt, um die Festplatten zu entschlüsseln. Sie sollte geheim sein, sicher gespeichert werden und nur denjenigen Personen zur Verfügung stehen, die eine Notfall-Wiederherstellung durchführen müssen.
  DLFDEMaster.cer ist die öffentliche Schlüsselkomponente des Hauptzertifikates (MSC) und wird automatisch für jede Installation verwendet.

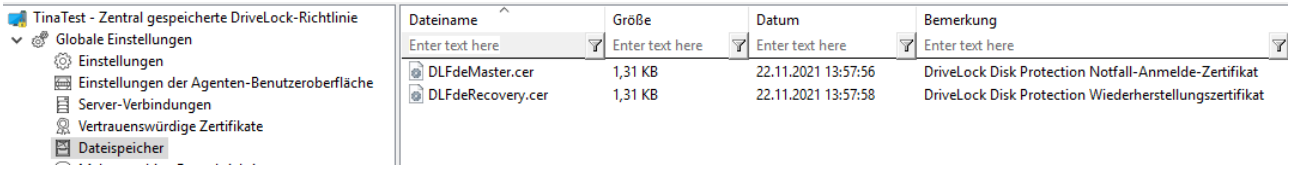
- **Wiederherstellungszertifikat (RSC = Recovery Support Certificate):**

  Die Dateien DLFDERecovery.cer und DLFDERecovery.pfx ergeben ein öffentliches/privates Schlüsselpaar.
  DLFDERecovery.pfx wird für das Notfall-Anmeldeverfahren verwendet. Sie sollte geheim sein, sicher gespeichert werden und nur denjenigen Personen zur Verfügung stehen, die eine Kennwort-Wiederherstellung durchführen (z.B. Helpdesk/Support Personal).

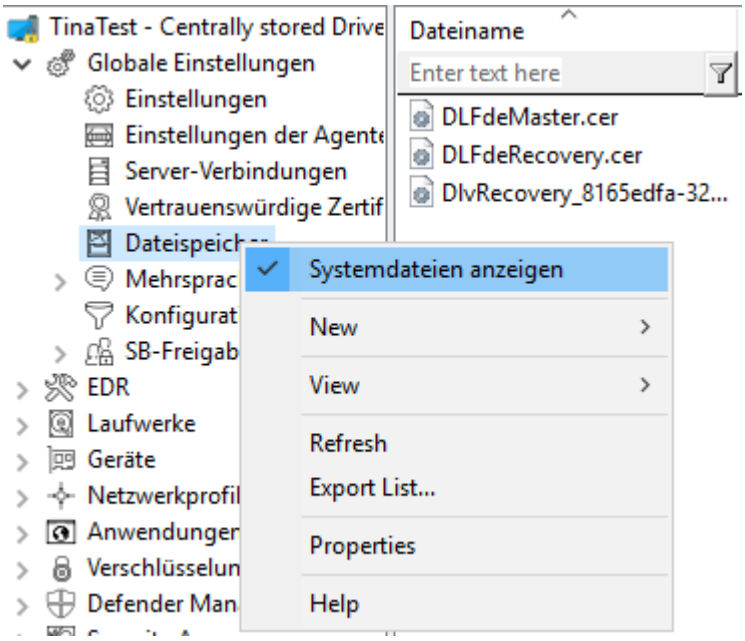
DLFDERecovery.cer ist die öffentliche Schlüsselkomponente des Wiederherstellungszertifikates (RSC) und wird automatisch für jede Installation verwendet.

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

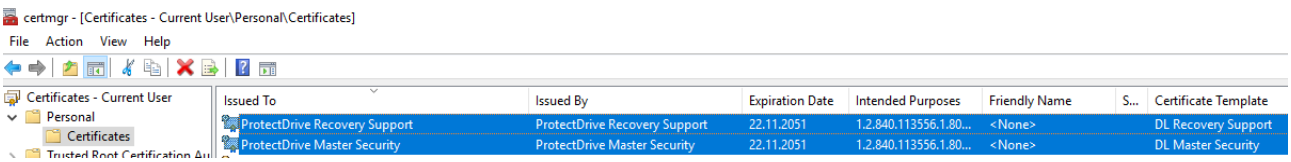
Sobald die Verschlüsselungszertifikate erzeugt wurden, zeigt die DriveLock Management Konsole die Erstellungszeit und das Datum an.



Beachten Sie, dass die Einstellung **Systemdateien anzeigen** aktiviert sein muss, damit diese Zertifikate angezeigt werden:



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



7.1.1.1 Verschlüsselungszertifikate erzeugen

Zunächst müssen die zentralen Zertifikate generiert werden, die für alle Wiederherstellungsmechanismen benötigt werden. Sie können diese zusätzlich zu den von DriveLock angebotenen Möglichkeiten beispielsweise auf einer Smartcard sichern.

Gehen Sie folgendermaßen vor:

1. Öffnen Sie im Richtlinien-Editor den Knoten **Verschlüsselung**.
2. Je nachdem, welche Ansicht Sie gewählt haben, gehen Sie entweder über die Taskpad-Ansicht zum Bereich **DriveLock Disk Protection** und wählen hier **Hauptzertifikate erzeugen...**. Oder Sie wählen direkt im Unterknoten **DriveLock Disk Protection** die Option **Verschlüsselungszertifikate**.
3. Im Dialog klicken Sie die Schaltfläche **Zertifikate erzeugen**. Folgen Sie dann den Anweisungen hier ab Schritt 3.

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

7.1.1.2 Wiederherstellungsschlüssel

Wiederherstellungsinformation werden standardmäßig in der Datenbank auf dem DriveLock Enterprise Service (DES) gespeichert. Wir empfehlen, diese Option aktiviert zu lassen.

Falls Sie jedoch auf dem Reiter **Wiederherstellung** eine der beiden anderen Optionen **Dateiserver (UNC-Pfad)** oder **Lokaler Ordner auf Agenten Computer (nicht empfohlen)** auswählen, werden die folgenden Dateien angelegt:

- **Recovery.env – Envelope-Datei für die Notfall-Anmeldung**

  Die Envelope-Datei wird sofort erstellt, nachdem der Agent die Disk Protection auf dem Client-Computer installiert hat, und zu dem angegebenen Ort gesendet. Die ZIP-Datei mit den EFS-Wiederherstellungs-Dateien wird erst erstellt und kopiert, nachdem alle Laufwerke vollständig verschlüsselt wurden.

- **DiskKeyBackup.zip – Diese ZIP Datei enthält die EFS-Wiederherstellungsdatei für das Recovery Verfahren zur Datenwiederherstellung**

  Die Wiederherstellungs-Dateien sollten entweder im DriveLock Enterprise Server oder einer zentralen Dateifreigabe gespeichert werden. Zusätzlich können die Dateien lokal auf dem Computer gespeichert werden, allerdings wird dies aus Sicherheits- und Wiederherstellungsgründen nicht empfohlen.

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

Hinweis: Jeder Client-Computer hat seine eigene entsprechende Envelope-Datei, die für die Notfall-Anmeldung verwendet werden muss. Wenn Sie Disk Protection so konfiguriert haben, dass die Datei automatisch auf eine zentrale Dateifreigabe abgelegt wird, beginnt der Dateiname mit dem Namen des Client-Computers (z.B. DE2319WX.Envelope.env).

7.1.2 Benutzerbezogene Agenteneinstellungen

Standardmäßig werden Benutzer der DriveLock Agenten von der Installation von bzw. Verschlüsselung mit Disk Protection informiert und ihr Client-Computer wird nach 30 Sekunden neu gestartet. Sie können diese Einstellungen bei Bedarf ändern.

Reiter Agenteneinstellungen

Sie können dabei auswählen, ob Benachrichtigungen angezeigt werden und genau differenzieren, wann diese im Benachrichtigungsfeld angezeigt werden: während der Konfiguration, während der Verschlüsselung und bzw. oder vor der Installation von Updates.

Die Option **Benutzerbenachrichtigungen anzeigen / Neustarts bestätigen** sowie die vier Optionen unterhalb sind standardmäßig aktiviert.

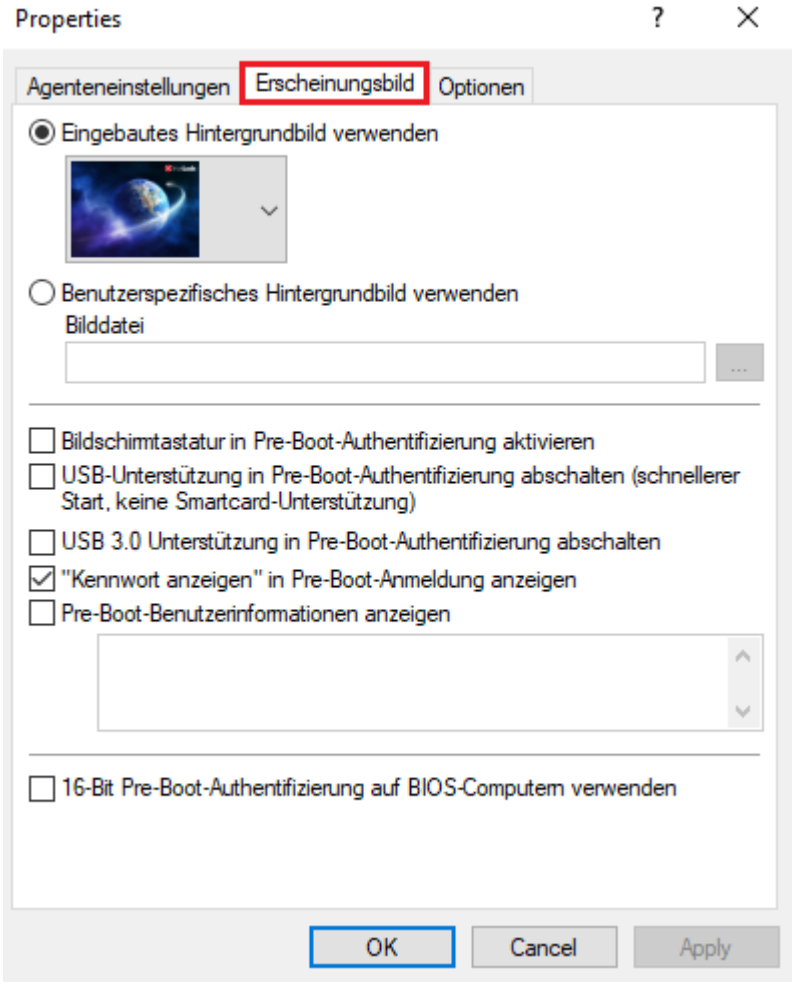
Wählen Sie die Option **Computer nicht neu starten (manueller Neustart erforderlich)**, wenn Sie diesen selbst steuern wollen. Sie können dann z.B. über einen Kommandozeilenbefehl nach der Installation ein eigenes Installationsskript starten.

Hierfür stehen zwei Optionen zur Auswahl:

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

Reiter Erscheinungsbild

Auf diesem Reiter geben Sie an, wie Disk Protection bzw. die DriveLock PBA bei den Endbenutzern angezeigt wird.



- **Eingebautes Hintergrundbild verwenden**: Disk Protection liefert bereits vorgefertigte Hintergrundbilder mit, aus denen Sie das gewünschte Bild für die Pre-Boot-Authentifizierung auswählen können.
- **Benutzerspezifisches Hintergrundbild verwenden**: Sie die Datei aus dem Richtliniendateispeicher oder aus dem Dateisystem auswählen, Format PNG, maximal 32 MB, optimale Auflösung 1024x768.
- **Bildschirmtastatur**: Mit Hilfe einer virtuellen Tastatur können Benutzereingaben auch ohne vorhandene reale Tastatur erfolgen
- **USB-Unterstützung**: Ist diese deaktiviert, kann die PBA schneller geladen werden. Allerdings funktionieren damit keine über die USB-Schnittstelle angeschlossenen Geräte, wie z.B. Maus oder Smartcard Leser

- **USB 3.0 Unterstützung**: Diese Option deaktiviert den Support von USB 3.0 Geräten innerhalb der PBA
- **Kennwort anzeigen**: Damit kann verhindert werden, dass ein eingegebenes Kennwort im Klartext angezeigt wird. Diese Option ist standardmäßig gesetzt.
- **Pre-Boot-Benutzerinformationen anzeigen**: Geben Sie im Textfeld eigene Benutzerinformationen ein, die dann innerhalb der PBA angezeigt werden, z.B. Hinweise zur Verwendung oder Ansprechpartner
- Die Option **16-Bit Pre-Boot-Authentifizierung auf BIOS-Computern verwenden** ist nur möglich, wenn Sie noch BIOS-Computer im Einsatz haben. Für die DriveLock Pre-Boot Authentifizierung unter UEFI-Systemen wird die 16-Bit PBA nicht mehr unterstützt.

Reiter Optionen

DriveLock Disk Protection-Logon-Benachrichtigungen anzeigen: Wählen Sie diese Option aus, wenn die Anmelde-Informationen der Pre-Boot Authentifizierung nach der Anmeldung in Windows im Benachrichtigungsfeld des Client-Computers angezeigt werden sollen.

Auf dem Client-Computer erscheint dann eine Nachricht mit detaillierten Informationen.

Hinweis: Die anderen Optionen in diesem Dialog sind ausschließlich für BIOS-Systeme relevant.

7.1.3 Einstellungen für die Verschlüsselung

In diesem Dialog stehen folgende Einstellungen zur Verfügung.

Auf dem Reiter **Allgemein**:

- Hier können Sie die Verschlüsselung mit Disk Protection aktivieren, in dem Sie die Option **Lokale Festplatten auf Agenten-Computern verschlüsseln** auswählen.
- Als **Verschlüsselungsalgorithmus** ist AES vorgegeben und kann so übernommen werden. Sie können zwischen verschiedenen Verschlüsselungs-Algorithmen auswählen, wir empfehlen AES 256-bit.
- Mit **Einstellungen pro Laufwerk konfigurieren** können Sie die Verschlüsselung für jedes Laufwerk separat bestimmen. Voreingestellt ist die Verschlüsselung aller lokalen Festplatten.

- Wenn Sie **FIPS-konforme Verschlüsselungsbibliothek verwenden** auswählen, wird die FIPS Bibliothek verwendet. Wenn diese Option nicht ausgewählt wird, ist die Performance besser und eine CC EAL-2 zertifizierte Nicht-FIPS-Bibliothek verwendet automatisch die Hardware-Unterstützung AES NI (Intel® Advanced Encryption Standard (AES) Instructions Set), sofern der Client dies unterstützt.
- Um allen Benutzern einen Warnhinweis anzuzeigen, der auf eine unvollständige Laufwerks-Verschlüsselung hinweist, kann die Option **Warnung anzeigen, wenn Festplatten nicht voll verschlüsselt sind** aktiviert werden.
- **Verschlüsselungspriorität**: Stellen Sie hier ein, mit welcher Rechnerleistung die Verschlüsselung durchgeführt wird. Standardmäßig ist der Wert **Normal** gesetzt. Bei der Einstellung **Hoch** werden andere Anwendungen möglicherweise langsamer ausgeführt.
- **Festplattenüberprüfung (ChkDsk) vor Verschlüsselung ausführen**: Verwenden Sie diese Option, um die Integrität des Dateisystems aller Laufwerke sicherzustellen, die Sie verschlüsseln wollen. Dabei werden alle fehlerhaften Sektoren repariert, damit Disk Protection diese verschlüsseln kann.
- Disk Protection verwaltet einen Speicher für einige BIOS Interrupt-Vektor-Adressen (nur Legacy BIOS). Das erlaubt es Disk Protection, potenzielle Angriffe zu erkennen, die durch das Ändern der Interrupt-Vektor-Adressen gestartet werden. Wenn es einen Unterschied zwischen der BIOS Interrupt-Vektor-Adresse und der zuvor gespeicherten Kopie erkennt, wird eine Fehlermeldung angezeigt.
  Wenn sich die Interrupt-Vektor-Adresse ändert (z.B. durch ein BIOS Update), wird der Fehler weiterhin an-gezeigt. Die System-Schutz-Gruppe stellt einen Mechanismus zur Verfügung, um berechtigte Änderungen, durch Aktualisierung der Kopie von Festplatten-, Tastatur- und Clock-Tick-Interrupt-Vektor-Adressen, zu akzeptieren.
  Über die Option **Interrupt-Vektor-Schutz vollständig deaktivieren** können Sie die Überprüfung der Interrupt-Vektoren komplett deaktivieren.
- Die Option **Erst verschlüsseln, wenn Pre-Boot-Anmeldung einmal erfolgreich war** kann aktiviert werden, um die Verschlüsselung der Festplatten so lange zu verzögern, bis sich ein Benutzer einmalig erfolgreich an der Pre-Boot Authentifizierung angemeldet hat und damit in der Benutzerdatenbank der PBA gespeichert wurde.
- Die Option **Bei Konf.änderungen Entschlüsselung um x Tage verzögern** zögert die Entschlüsselung um eine bestimmte Anzahl an Tagen hinaus. Dies kann sinnvoll sein, um die Client-Computer und deren Benutzer auf die Entschlüsselung entsprechend vorbereiten zu können.

Als Standardwert ist ein Wert von **3** Tagen vordefiniert. Dieser Wert bietet einen zusätzlichen Schutz vor Fehlkonfigurationen. Wenn Sie sofort eine Entschlüsselung durchführen wollen, ändern Sie die Einstellung auf 0 Tage.

Auf dem Reiter **Wiederherstellung**:

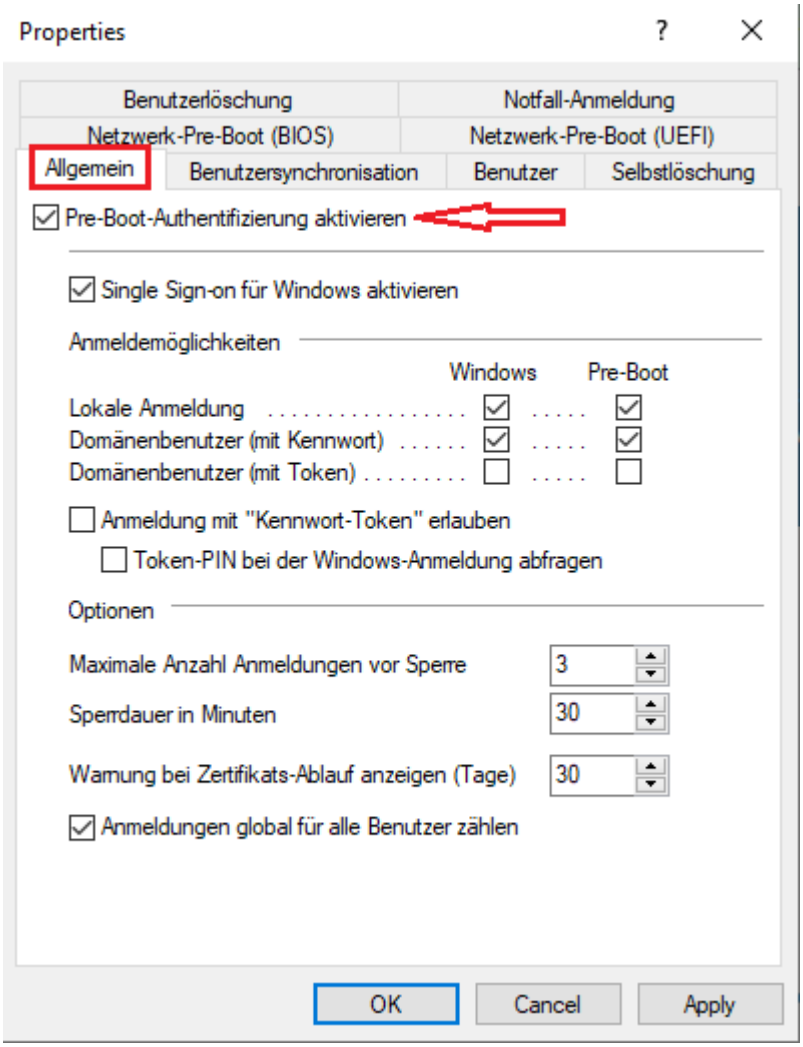
Hier geben Sie an, wo der Wiederherstellungs-Schlüssel des DriveLock Agenten für das Challenge-Response-Verfahren gespeichert werden soll.

7.1.4 Einstellungen für die Pre-Boot-Authentifizierung

7.1.4.1 Allgemein

In den **Einstellungen für die Pre-Boot-Authentifizierung** können Sie die Pre-Boot-Authentifizierung für DriveLock Agenten aktivieren, die mit Disk Protection geschützt werden.

Auf dem Reiter **Allgemein** wählen Sie hierzu die Option **Pre-Boot-Authentifizierung aktivieren**.



Um Zugriff auf ein durch Disk Protection geschütztes System zu bekommen, ist eine Authentifizierung sowohl auf Ebene der Pre-Boot-Authentifizierung als auch auf der Windows Zugriffsebene notwendig. Im Single Sign-on Modus muss sich ein Endbenutzer für beide Ebenen (Pre-Boot und Windows) nur einmal anmelden. Die Option **Single Sign-on für Windows** aktivieren ist deshalb standardmäßig gesetzt.

Dem Benutzer stehen für die Pre-Boot- und Windows-Authentifizierung eine Kombination aus lokalen Benutzern, Domänenbenutzer (mit Kennwort) und Domänenbenutzer (mit Token) zur Verfügung. Auch hier sind standardmäßig die beiden oberen Optionen gesetzt.

- **Lokale Anmeldung**: Diese voreingestellte Methode erlaubt es lokalen Windows-Benutzern, sich mit ihrem lokalen Windows Benutzernamen, Kennwort und lokalen Systemnamen am System zu authentisieren.
- **Domänenbenutzer (mit Kennwort)**: Diese Methode erlaubt es Windows Domänen-Benutzern, sich mit ihrem Windows Domänen-Benutzernamen, Kennwort und Domänennamen am System zu authentisieren.
- **Domänenbenutzer (mit Token)**: Diese Methode erlaubt es Windows Domänen-Benutzern, eine Smartcard/Token und PIN für die Authentifizierung zu benutzen.
- **Anmeldung mit "Kennwort-Token" erlauben**: Diese Methode erlaubt die Pre-Boot-Authentifizierung für einen Kennwort-Token Benutzer. Wenn diese Option markiert ist, muss mindestens noch eine Windows Authentifizierung ausgewählt werden.

  Hinweis: Stellen Sie sicher, dass es ein gültiges Token für beide PBA und Windows-Anmeldung (Entsperren) gibt, bevor Disk Protection nur für Token Zugriff konfiguriert wird.

- **Fehlgeschlagene Anmeldungen global für alle Benutzer zählen** ist voreingestellt und bewirkt, dass Fehlversuche unabhängig vom angegebenen Benutzer hochgezählt werden.

  Hinweis: Nach einer bestimmten Anzahl von fehlerhaften Anmeldungen kann ein Benutzer für eine bestimmte Zeit gesperrt werden, um das System vor einer Brute-Force-Attacke mit automatischen Anmelde-Skripten zu schützen. Ändern Sie die Standard-Werte gemäß Ihren Unternehmens-Sicherheitsrichtlinien.

- Wenn man Zertifikate für die Authentifizierung benutzt, kann man auch die Anzahl der

Tage festlegen, wann Disk Protection den Benutzer informiert, bevor sein Zertifikat ausläuft.

Sobald eine Richtlinie mit dieser Einstellung auf den DriveLock Agenten wirksam wird, wird die PBA dort aktiviert und dem Endbenutzer wird ein entsprechende Dialog angezeigt.

7.1.4.2 Netzwerk-Pre-Boot (BIOS)

Hinweis: Beachten Sie, dass ab Version 2022.2 die DriveLock Legacy BIOS Pre-Boot Authentifizierung nicht mehr unterstützt wird und aus dem Produkt entfernt wird. Bei der Installation eines Agenten der Version 2022.2 wird geprüft, ob eine aktive Legacy BIOS PBA auf dem System vorhanden ist. In diesem Fall wird eine Aktualisierung bzw. Installation des Agenten nicht durchgeführt.

Für bestimmte Legacy-BIOS Systeme bietet Disk Protection eine netzwerkfähige Pre-Boot-Authentifizierung an, die automatisch erkennen kann, ob sich der Rechner in einem vordefinierten Unternehmensnetzwerk befindet und eine Anmeldung an der PBA deaktiviert (Auto-Boot).

Diese Funktionalität steht nur für bestimmte Systeme Verfügung und sollte nur in Zusammenarbeit einem Mitarbeiter des DriveLock Professional Service Teams aktiviert werden.

7.2 Entschlüsselung

Die Entschlüsselung von Festplatten kann aufgrund folgender Gründe starten:

- Die Option **Lokale Festplatten auf Agenten-Computer verschlüsseln** wird innerhalb der Richtlinie deaktiviert (siehe unten)
- Die Zuweisung der Richtlinie mit den Disk Protection-Einstellungen wird entfernt bzw. aufgehoben
- Die Lizenzoption Disk Protection innerhalb einer zugewiesenen Richtlinie wird entfernt

Hinweis: Der Entschlüsselungsprozess lässt sich, ebenso wie der Verschlüsselungsprozess, auch im DriveLock Operations Center (DOC) nachverfolgen.

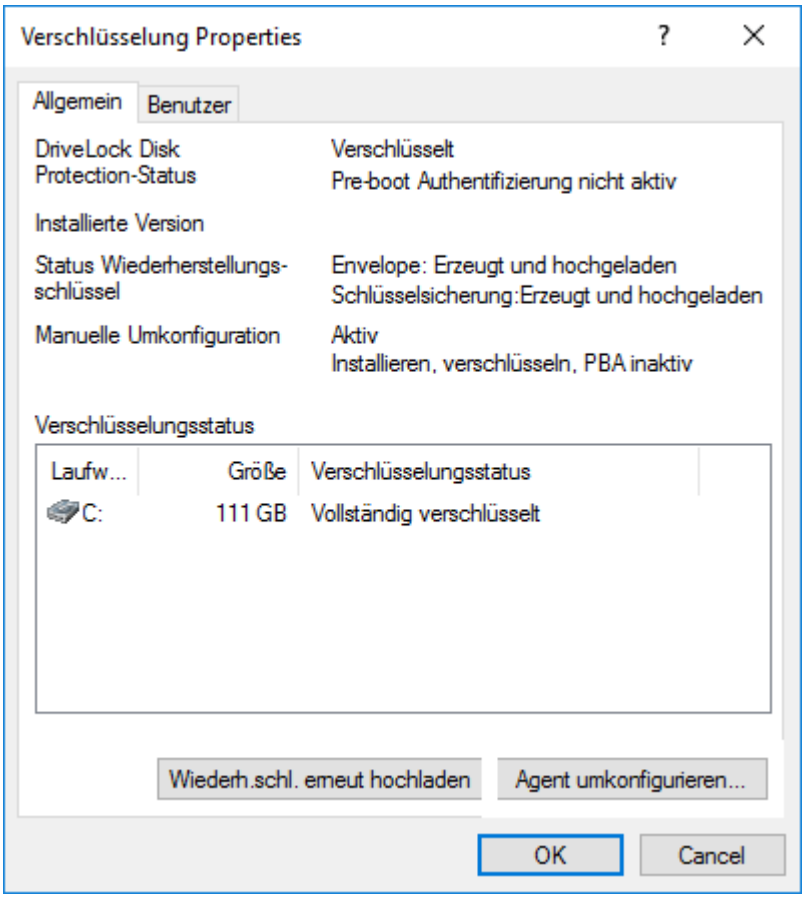
Um die Entschlüsselung bereits verschlüsselter Festplatten anzustoßen, gehen Sie wie folgt vor:

1. Öffnen Sie die entsprechende Disk Protection-Richtline.
2. Öffnen Sie den Dialog **Einstellungen für die Verschlüsselung** und hier den Reiter **Allgemein**.
3. Entfernen Sie das Häkchen bei der Option **Lokale Festplatten auf Agenten-Computern verschlüsseln**.
4. Wenn Sie sofort eine Entschlüsselung durchführen wollen, ändern Sie die Einstellung **Bei Konf.änderungen Entschlüsselung um x Tage verzögern** auf 0 Tage.
5. Bestätigen Sie Ihre EInstellung.
6. Auf dem DriveLock Agenten wird die Entschlüsselung mit entsprechenden Meldungen durchgeführt.

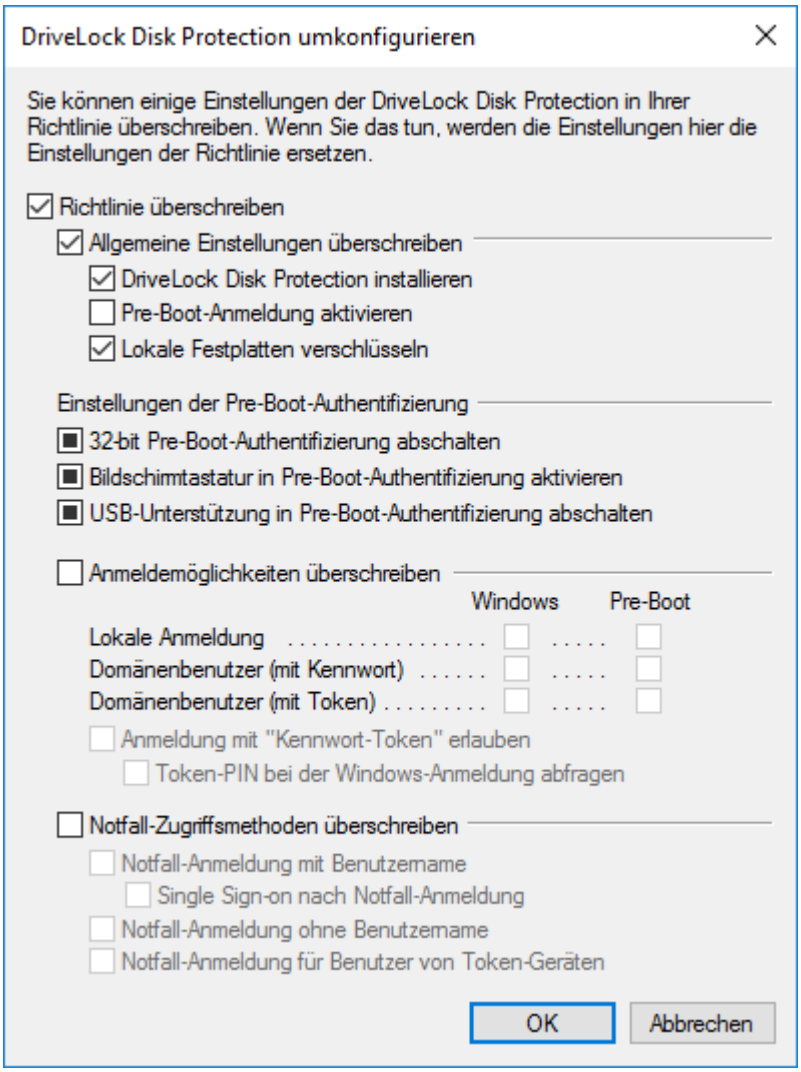
7.3 Richtlinie überschreiben (Disk Protection)

Wenn Sie Änderungen an der Disk Protection Konfiguration nur auf ganz bestimmten Computern vornehmen möchten (z.B. Deinstallation von Disk Protection, Entschlüsselung der Festplatten), kann unabhängig von der zentralen Konfiguration die Einstellung speziell für einen einzelnen Agenten überschrieben werden.

Dies erreichen Sie mit Hilfe der Agenten-Fernkontrolle. Verbinden Sie sich zuerst mit einem DriveLock Agenten und wählen aus dem Kontextmenü **DriveLock Disk Protection Eigenschaften**.



Klicken Sie auf **Agent umkonfigurieren**.



Aktivieren Sie **Richtlinie überschreiben**, um abweichend von der zentralen Richtlinie rechnerspezifische Einstellungen zu konfigurieren. Die gewählten Einstellungen gelten nur für den gerade verbundenen Computer.

Welche Benutzer in der PBA des Rechners hinterlegt sind, sehen Sie auf dem Reiter **Benutzer**. Sie können hier einzelne Benutzer hinzufügen oder löschen.

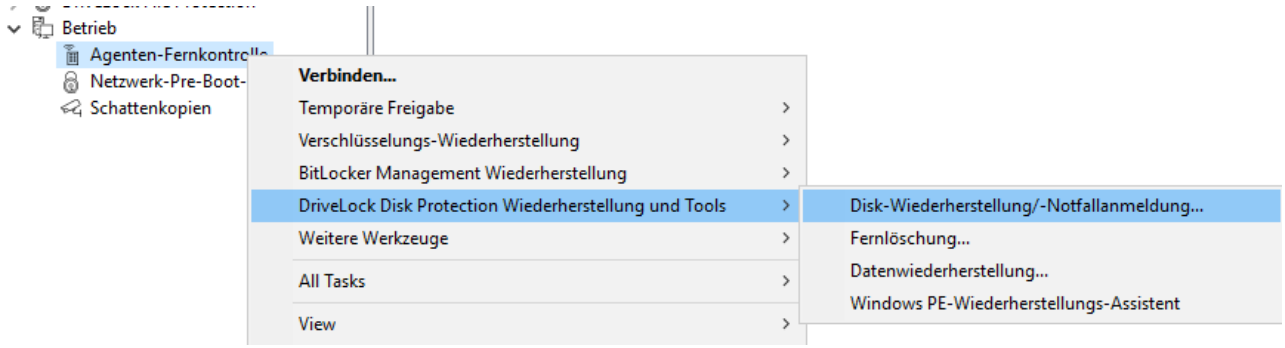
7.4 DriveLock Disk Protection Wiederherstellung und Tools

Disk Protection deckt zwei verschiedene Wiederherstellungsverfahren ab:

- Notfall-Anmeldeverfahren
  Die Notfall Anmeldeverfahren werden angewendet, wenn ein Benutzer nicht mehr in der Lage ist, sich an der Pre-Boot-Authentifizierung anzumelden (z.B. der Benutzer hat sein Passwort oder PIN vergessen).
- Wiederherstellung verschlüsselter Laufwerke (Daten)

Die Wiederherstellung von Laufwerken wird notwendig, wenn auf lokale Laufwerke nicht mehr zugegriffen werden kann. Dies ist z.B. dann der Fall, wenn Datensektoren eines Laufwerks defekt sind und man sich nicht mehr an Windows anmelden kann.

Beide Verfahren werden über den Wiederherstellung-Assistenten durchgeführt. Rechtsklicken Sie im Knoten **Betrieb** auf **Agenten-Fernkontrolle** und wählen Sie dann im Kontextmenü **DriveLock Disk Protection-Wiederherstellung/-Notfallanmeldung** aus.



7.4.1 Diagnoseinformationen speichern

Wenn DriveLock Disk Protection installiert ist, sendet der DriveLock Agent das Installationsprotokoll zum DriveLock Enterprise Service. Sollte die Disk Protection-Installation fehlgeschlagen sein, können Sie die Protokolldatei aus der DriveLock Datenbank laden und ansehen, um weitere Details zum aufgetretenen Fehler zu erhalten.

Gehen Sie folgendermaßen vor:

1. Wählen Sie im Wiederherstellungs-Assistent die Option **Diagnoseinformationen speichern** und **DriveLock Enterprise Service** aus.
2. Wählen Sie im nächsten Dialog die DES-Serververbindung aus der Auswahlliste aus.
3. Um einen registrierten Agenten in der DriveLock-Datenbank zu finden, geben Sie den Computernamen oder einen Teil des Namens ein und klicken auf Suchen. Disk Protection zeigt alle registrierten Computer an, die den Suchtext als Teil ihres Computernamens haben. Um alle registrierten Computer zu finden, lassen Sie das Textfeld leer und klicken auf Suchen.
4. Wählen Sie den entsprechenden Computer aus der Liste aus.
5. Im nächsten Dialog wählen Sie den Pfad aus, wo die Diagnosedatei abgespeichert werden soll. Klicken Sie auf Weiter, um die Datei aus der DriveLock-Datenbank zu empfangen.
6. Nachdem Sie die Datei erhalten haben, klicken Sie auf Fertigstellen. An dem ausgewählten Pfad wurde eine ZIP-Datei abgelegt, die Sie nun entpacken können.

7.4.2 Einstellungen für die Notfall-Anmeldung (Challenge-Response)

Die Notfall-Anmeldeverfahren werden in den Einstellungen für die Pre-Boot-Authentifizierung konfiguriert.

Zur Unterstützung des Endbenutzers bei der Notfall-Anmeldung gehen Sie folgendermaßen vor:

1. Öffnen Sie den Wiederherstellungs-Assistenten.
2. Wählen Sie auf der ersten Seite die Option **Notfall-Anmeldung**. Wenn Ihre Wiederherstellungs-Schlüssel zum DriveLock Enterprise Service gesendet werden, lassen Sie die Standardeinstellung **DriveLock Enterprise Service**. Wenn Sie den Pfad später zu den benötigten Wiederherstellungs-Schlüsseln angeben möchten, wählen Sie **Wiederherstellungsdateien (von Agenten-Computer kopiert)** aus.
3. Für das Notfall-Anmeldeverfahren benötigen Sie den privaten Schlüssel des Wiederherstellungs-Zertifikates. Im zweiten Dialog geben Sie den Speicherort an, entweder Windows-Zertifikatsstore, eine Smartcard oder eine PFX-Datei zusammen mit dem jeweiligen Kennwort. Weitere Informationen zu Zertifikaten finden Sie hier. Sofern Sie eine Smartcard verwenden, werden Sie abhängig von der verwendeten Karte aufgefordert, diese einzulegen und auszuwählen.
4. Im dritten Dialog wird eine Liste der Computer angezeigt, aus der Sie den wiederherzustellenden Computer auswählen. Setzen Sie ein Häkchen bei der Option **nur den neuesten Eintrag pro Computer zeigen**. Klicken Sie **Weiter**.
5. Als nächstes erscheint die Seite zur Eingabe des Anforderungs- bzw. Wiederherstellungscodes des Benutzers.

   Hinweis: Weitere Informationen zur Interaktion zwischen Administrator und Endbenutzer finden Sie hier.

   Geben Sie den Code in die entsprechenden Felder ein (siehe Abbildung). Sie können optional den Namen des Benutzers angeben.

   Achtung: Zwingend erforderlich ist jetzt der Wiederherstellungscode, den Ihnen der Benutzer übermitteln muss.

6. Klicken Sie **Weiter**, um den Antwortcode generieren zu lassen.

7. Teilen Sie dem Benutzer der **Antwortcode** mit.
8. Klicken Sie **Fertigstellen**.

7.4.3 Wiederherstellung verschlüsselter Laufwerke

Die Wiederherstellung von Laufwerken ist nötig, wenn auf lokale Laufwerke nicht mehr zugegriffen werden kann (z.B. wenn Datensektoren des Laufwerkes defekt sind).

Um ein verschlüsseltes Laufwerk wiederherzustellen (zu entschlüsseln), muss man die folgenden vier Schritte ausführen:

1. Erstellen Sie die Wiederherstellungsdateien
2. Kopieren Sie alle für die Entschlüsselung notwendigen Dateien auf einen USB Wechseldatenträger oder auf die Recovery-CD
3. Booten Sie den Rechner mit der Recovery-CD
4. Benutzen Sie die Wiederherstellungsdateien und -tools, um die gewünschte(n) Festplatte(n) auf dem betroffenen Computer zu entschlüsseln.

7.4.3.1 Disk-Schlüssel-Wiederherstellung

Gehen Sie folgendermaßen vor:

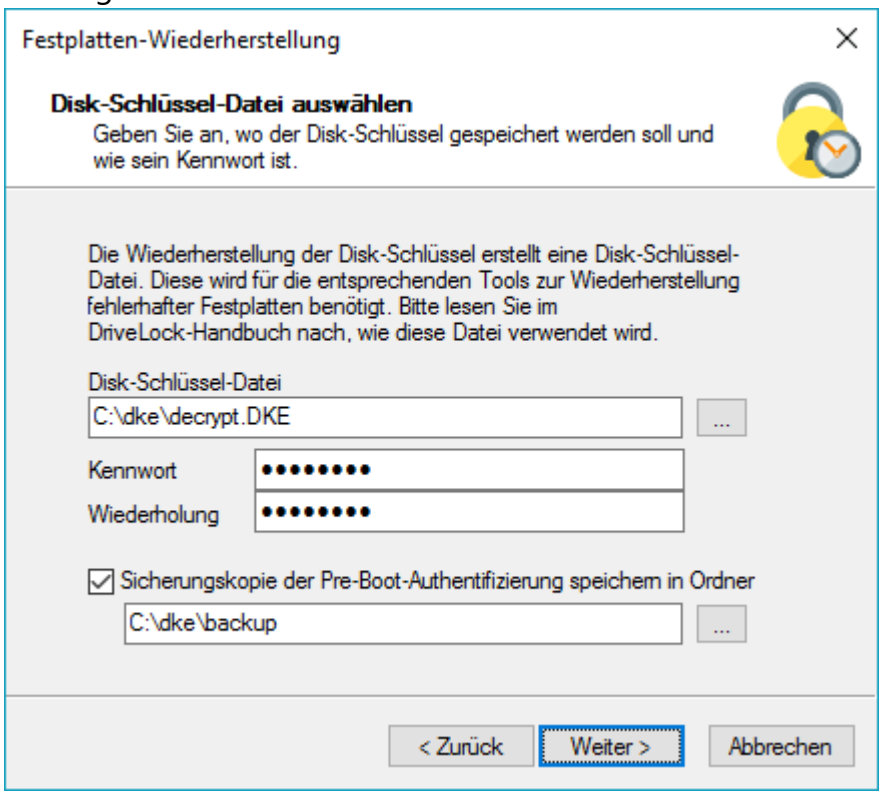
1. Wählen Sie die Option **Disk-Schlüssel-Wiederherstellung** als Wiederherstellungsmethode.
2. Wenn Sie Disk Protection so konfiguriert haben, dass die Client-Wiederherstellungsschlüssel zum DriveLock Enterprise Service gesendet werden, wählen Sie die Option **DriveLock Enterprise Service** aus. Wenn Sie den Pfad zu den benötigten Wiederherstellungsschlüsseln später angeben möchten, wählen Sie **Wiederherstellungsdateien (von Agenten-Computer kopiert)** aus.
3. Im nächsten Dialog wählen Sie aus, wo die Zertifikate/Wiederherstellungsschlüssel gespeichert sind. Entweder geben Sie den Pfad zur Datei DLFDEMaster.pfx an und dazu das entsprechende Kennwort (Option **Dateisystem**). Alternativ können Sie auch eine **Smartcard** verwenden, auf der zuvor die Zertifikatsinformationen gespeichert wurden. Wurden die Zertifikatsinformationen mit dem privaten Schlüssel in den lokalen Zertifikatsspeicher des aktuell angemeldeten Benutzers importiert, können Sie auch die erste Option **Windows-Zertifikatsspeicher** auswählen.
4. Wählen Sie im nächsten Dialog entweder die Agenten mit DriveLock Disk Protection aus oder geben Sie die Datei für die Wiederherstellungsinformationen an.

Hinweis: Jeder Client-Computer hat seine eigene entsprechende EFS-Wiederherstellungsdatei, die für die Laufwerks-Wiederherstellung verwendet werden muss. Wenn Sie Disk Protection so konfiguriert haben, dass die Datei automatisch auf eine zentrale Dateifreigabe abgelegt wird, beginnt der Dateiname mit dem Namen des Client-Computers (z.B. DE2319WX.Backup.-zip). Die EFS-Wiederherstellungsdateien werden automatisch vom DriveLock Agenten erzeugt, sobald die Festplattenverschlüsselung beginnt.

5. Im nächsten Dialog geben Sie an, wo der Disk-Schlüssel gespeichert wird. Es ist erforderlich, dass Disk Protection einen speziellen Disk-Schlüssel erstellt. Geben Sie einen Dateinamen und Pfad an. Alternativ können Sie den Pfad und Dateinamen manuell angeben.

   Hinweis: Stellen Sie sicher, die korrekte Dateiendung (*.dke) anzugeben.

   Geben Sie ein Kennwort an, um den Zugriff auf diese Datei abzusichern. Das Kennwort muss mindestens sechs Zeichen lang sein. Es wird später für die Wiederherstellung benötigt.



   Wählen Sie die Option **Sicherungskopie der Pre-Boot-Authentifizierung speichern in Ordner** um alle Wiederherstellungsdaten, die in der DriveLock Datenbank gespeichert sind, in eine Backup.zip zu exportieren.

6. Klicken Sie auf Weiter, um den Disk-Schlüssel zu erstellen.
   Sofern Sie eine Smartcard verwenden, werden Sie nun aufgefordert, die PIN für den Zugriff auf die Karte einzu-geben.
7. Jetzt können Sie die erstellte Datei auf ein USB Laufwerk oder die Recovery-CD kopieren, um diese in den nächsten Schritten zu verwenden.

7.4.3.2 Erstellen eines Wiederherstellungsmediums

Um ein System wiederherzustellen, das nicht mehr gestartet werden kann, wird eine bootfähiges Wiederherstellungsmedium (oder Recovery CD) für den Systemstart benötigt.

Hinweis: Sie benötigen nur ein Wiederherstellungsmedium für Ihre Systemumgebung, da die individuelle Wiederherstellungsdatei auf einen weiteren USB-Stick kopiert wird.

Bevor Sie den Assistenten starten, müssen folgende Bedingungen erfüllt sein:

- Sie besitzen auf Ihrem Rechner administrative Rechte, um das Windows Assessment and Deployment Kit (ADK) zu installieren.

  Achtung: Das ADK muss installiert sein, um mit dem Windows PE-Wiederherstellungs-Assistenten ein Wiederherstellungsmedium ('recovery image') erstellen zu können.

- Auf Ihrem Rechner ist die aktuelle DriveLock Management Konsole installiert.
- Ein USB-Stick (mind. 1GB) oder eine beschreibbare CD für das Windows PE Wiederherstellungsmedium liegt bereit.

7.4.3.2.1 Windows PE-Wiederherstellungs-Assistent

Rufen Sie den Assistenten über die Kontextmenübefehle **DriveLock Disk Protection Wiederherstellung und Tools** und dann **Windows PE-Wiederherstellungs-Assistent** im Unterknoten Agenten-Fernkontrolle auf. Der Assistent steht nur in englischer Sprache zur Verfügung.

1. Im ersten Dialog klicken Sie lediglich auf **Weiter**.
2. Im zweiten Dialog akzeptieren Sie die Lizenz.
3. Im dritten Dialog stellen Sie sicher, dass alle Vorbedingungen erfüllt und mit einem grünen Haken versehen sind.

4. Im vierten Dialog geben Sie das Verzeichnis an, in das die Ausgabedateien geschrieben werden sollen, wählen die Sprache und die Zielarchitektur der zu verwendenden Windows PE Umgebung aus.

   Achtung: Für UEFI Systeme ist zwingend die Architektur amd64 auszuwählen.

   Sie können nun noch zusätzliche Treiber und weitere Tools angeben, die zur Windows PE Umgebung hinzugefügt werden sollen. Das können weitere Festplattentreiber oder jegliche andere Tools sein, die ohne eine Installation ausgeführt werden können (z.B. Antivirus-Scanner, Backup-Tools, weitere Dritt-Hersteller-Werkzeuge, usw.).

5. Im folgenden Dialog wählen Sie aus, ob Sie eine bootfähige ISO-Datei oder einen bootfähigen USB-Stick erstellen möchten. Wenn Sie keine Auswahl treffen, wird lediglich eine Dateistruktur erzeugt, die Sie selbst manuell auf ein bootfähiges Medium kopieren müssen. Starten Sie den automatischen Vorgang, indem Sie **Create WinPe image** klicken. Sobald der Vorgang abgeschlossen ist, erscheint eine entsprechende Meldung.
6. Wenn der Vorgang beendet ist, werden Ihnen die Links zum jeweiligen Verzeichnis angezeigt. Klicken Sie **Finish**, um den Assistenten zu beenden.

Die so erzeugte Wiederherstellungs-CD enthält nun alle für die Wiederherstellung notwendigen Werkzeuge, Treiber und Wiederherstellungsdateien, die für einen Zugriff notwendig sind.

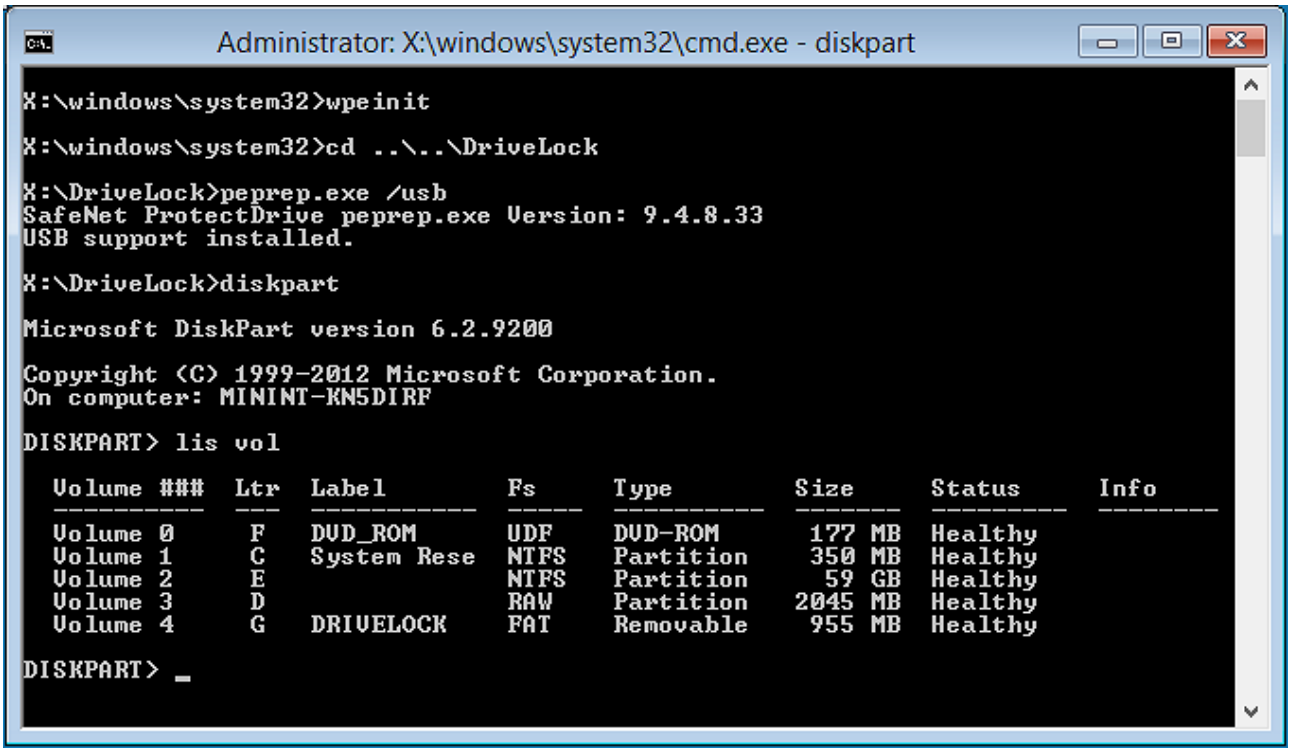
7.4.3.3 Wiederherstellung der Festplatte

Bevor Sie die Wiederherstellung starten können, stellen Sie sicher dass folgende Bedingungen erfüllt sind:

- Die notwendige *.dke-Datei für den benötigten Computer wurde erstellt und auf einen USB-Stick kopiert
- Ein bootfähiges Windows PE Wiederherstellungsmedium wurde erstellt

Booten Sie den Rechner vom Wiederherstellungsmedium.

Danach sehen Sie ein Kommandozeilen-Fenster mit einer Liste der verfügbaren Laufwerke (Volumes). Um diese Liste wieder anzuzeigen, verwenden Sie diesen Befehl: `echo lis vol | diskpart`



Verschlüsselte Laufwerke werden in der Spalte Fs als RAW angezeigt. Merken Sie sich nun den Laufwerksbuchstaben des USB-Sticks, der die Wiederherstellungsdatei enthält (ggf. den Stick einstecken und die Liste neu anzeigen lassen).

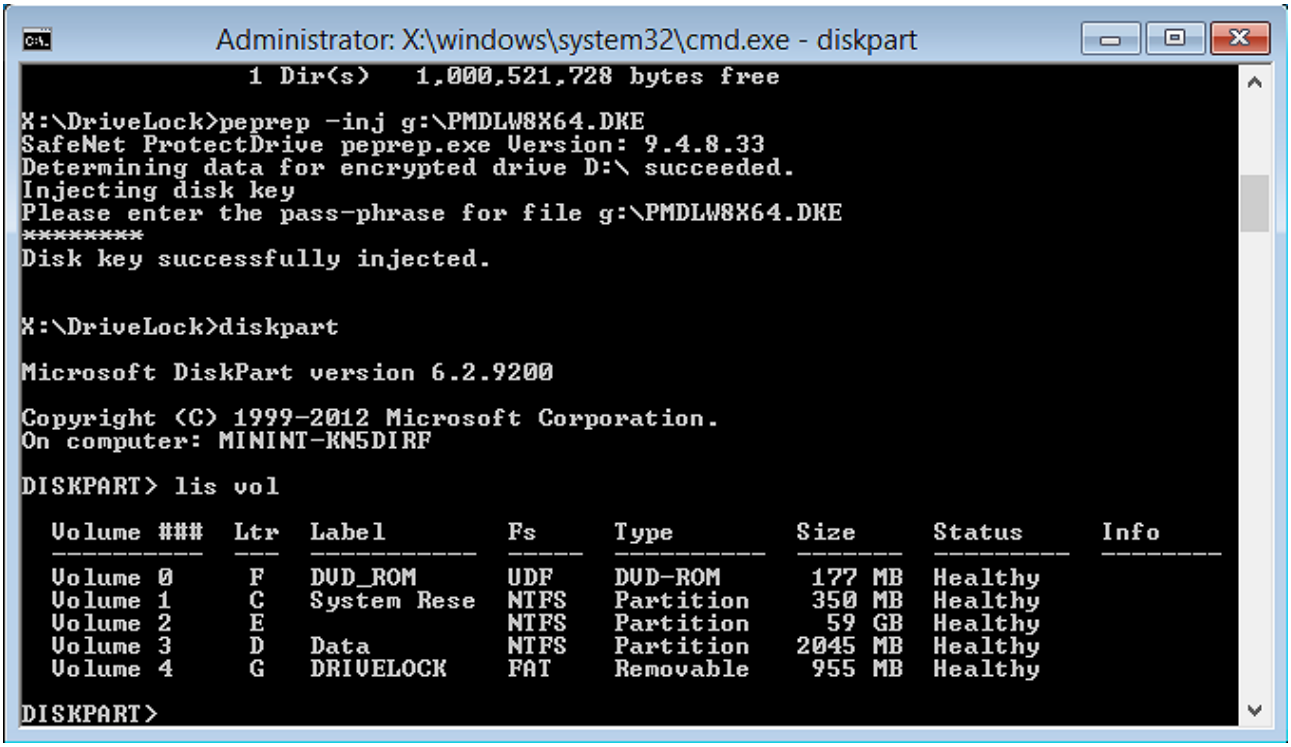
Geben Sie den Befehl `cd X:\DriveLock` ein.

Der folgende Befehl dient dazu, den Wiederherstellungsschlüssel für die Entschlüsselung dem System bekannt zu machen:

```
peprep -inj <USB drive letter>:\<path to disk key file>
```

In diesem Beispiel lautet der Befehl also `peprep -inj G:\PMDLW8X84.DKE`. Geben Sie nun das Kennwort ein, welches Sie bei der Erstellung der DKE-Datei verwendet haben.

Führen Sie den Befehl `echo lis vol | diskpart` erneut aus, um zu sehen ob der Wiederherstellungsschlüssel erfolgreich hinzugefügt wurde.



War die Aktion erfolgreich, wird das Laufwerk nicht mehr als RAW angezeigt.

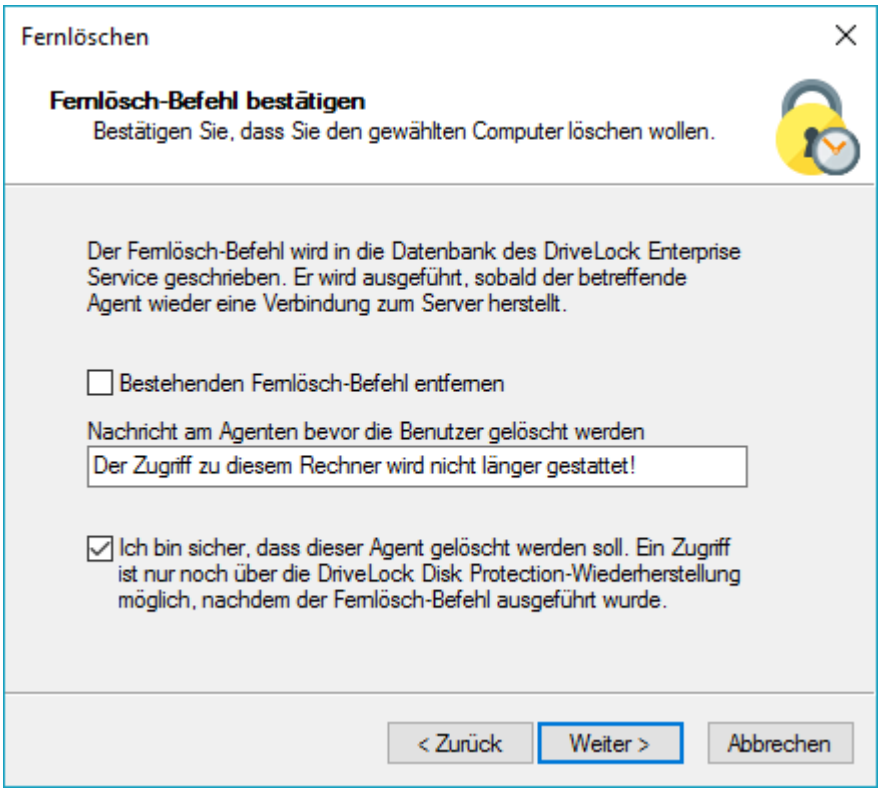
Geben Sie `Exit` ein, um DISKPART zu verlassen.

Nun haben Sie Zugriff auf das Laufwerk (sofern kein schwerwiegenderer Fehler vorliegt) und können wichtige Dateien kopieren oder versuchen, die Festplatte zu reparieren.

7.4.4 Fernlöschung

Die DriveLock PBA kann von einem Administrator gelöscht werden. Diese Fernlöschung erfolgt durch einen Rechts-Klick in der DriveLock Management Konsole auf **Betrieb** und dann **Agenten-Fernkontrolle** im Kontextmenü **Disk Protection Wiederherstellung und Tools** mit dem Kontextmenübefehl **DriveLock Disk Protection Fernlöschung**.

Für die Aktivierung der Fernlöschung benötigen Sie den privaten Schlüssel des Wiederherstellungs-Zertifikates. Geben Sie den Pfad zur Datei DLFDERecovery.pfx und das korrekte Kennwort ein. Anschließend wählen Sie den Computer aus, den Sie löschen möchten. Im nächsten Dialog müssen Sie den **Fernlösch-Befehl bestätigen**. Die vorgenommenen Einstellungen werden aktiviert, sobald sich der Computer mit dem DES verbindet. Damit die Fernlöschung auch außerhalb des Firmennetzwerkes funktioniert, muss der DES aus dem Internet erreichbar sein.



Konfigurieren sie die Einstellungen wie im Dialog angezeigt.

Markieren Sie **Bestehenden Fernlösch-Befehl entfernen**, um einen zuvor erteilten Fernlösch-Befehl zu widerrufen (sofern die PBA Datenbank noch nicht gelöscht ist).

Index

A

Authentifizierungstyp 28, 41

C

Copyright 204

D

Datenpartition 29

E

Entschlüsselung 18, 22, 38

F

Festplatten 9, 18, 28, 37, 41-42, 53

H

Hardware-Verschlüsselung 19

I

Index 202

K

Kennwortoptionen 31, 41

P

Pre-Boot-Authentifizierung 28, 41, 54, 57

privater Schlüssel 14, 24

S

Systempartition 29, 42, 47, 57

V

Verschlüsselung 9, 13, 18, 32, 41, 46, 54-55

Verschlüsselungsalgorithmus 19, 42

Verschlüsselungsmethoden 19

Verschlüsselungszertifikate 9, 13, 41

W

Wiederherstellung 13-14, 23, 42

Wiederherstellungsschlüssel 47

Z

Zertifikatsspeicher 13, 47

Zuweisung 54

Copyright