



DriveLock BitLocker Management

Dokumentation 2021.2

DriveLock SE 2021



Inhaltsverzeichnis

1 DRIVELOCK BITLOCKER MANAGEMENT	6
1.1 Allgemeines	6
1.1.1 Systemanforderungen	6
1.1.2 Algorithmen für DriveLock BitLocker Management	9
1.1.3 BitLocker Management lizenzieren	10
1.2 Richtlinienkonfiguration von BitLocker	12
1.2.1 Verschlüsselungseinstellungen	12
1.2.1.1 Verschlüsselungszertifikate	12
1.2.1.1.1 Verschlüsselungszertifikate erzeugen	13
1.2.1.2 Benutzerbezogene Agenteneinstellungen	15
1.2.1.3 Einstellungen für die Verschlüsselung	17
1.2.1.3.1 Reiter Allgemein	17
1.2.1.3.2 Reiter Verschlüsselungsschutz	20
1.2.1.3.3 Reiter Wiederherstellung	22
1.2.1.3.4 Reiter Ausführungsoptionen	24
1.2.1.4 Einstellungen für die Pre-Boot-Authentifizierung	27
1.2.1.4.1 Reiter Authentifizierungstyp	27
1.2.1.4.2 Reiter Kennwortoptionen	30
1.2.1.5 Änderungen der lokalen PBA-Konfiguration zulassen	32
1.2.1.6 PBA-Tastatortreiber auswählen	32
1.2.1.7 SmartCard-Treiber in PBA laden	33
1.2.2 Entschlüsselung	34
1.2.2.1 Verschlüsselte Festplatten entschlüsseln	34
1.2.3 Richtlinie überschreiben (BitLocker)	36
1.3 Beispielkonfiguration	38
1.4 Wiederherstellung	39

1.4.1 Wiederherstellung verschlüsselter Festplatten	39
1.4.2 Vorgehensweise zur Wiederherstellung	41
1.5 Übernahme	45
1.5.1 Übernahme bestehender BitLocker-Umgebungen	45
1.5.2 Nachträgliche Anpassung von BitLocker-Richtlinien	46
1.6 DriveLock Agent	48
1.6.1 Anmeldung an BitLocker	48
1.6.2 BitLocker Management auf Client-Computern (DriveLock Agent)	48
1.6.3 Verschlüsselung auf Client-Computern durchführen	49
1.6.3.1 Verschlüsselung verzögern	51
1.6.4 Datenpartition mit vorhandenem BitLocker übernehmen	53
1.7 BitLocker-Aktionen nachverfolgen	56
2 DRIVELOCK PRE-BOOT-AUTHENTIFIZIERUNG	57
2.1 Richtlinienkonfiguration der Pre-Boot-Authentifizierung	58
2.1.1 DriveLock PBA lizenzieren	58
2.1.2 Einstellungen für die Pre-Boot-Authentifizierung	58
2.1.2.1 Authentifizierungstyp	58
2.1.2.2 Anmelde-Methoden	60
2.1.2.3 Benutzer	61
2.1.2.4 Benutzersynchronisation	61
2.1.2.5 Benutzerlöschung	62
2.1.2.6 Erscheinungsbild	62
2.1.2.7 Netzwerk-Pre-Boot (UEFI)	62
2.1.2.8 Notfall-Anmeldung	62
2.1.2.9 Selbstlöschung	63
2.1.3 Richtlinie überschreiben (DriveLock PBA)	64
2.1.4 PBA-Einstellungen im DriveLock Operations Center (DOC)	66

2.2	Netzwerk-Pre-Boot-Authentifizierung (UEFI)	67
2.2.1	Netzwerk-Pre-Boot (UEFI)	68
2.2.2	Anwendungsfall 1: Automatische Anmeldung	71
2.2.3	Anwendungsfall 2: Netzwerkanmeldung für alle AD-Benutzer	73
2.2.4	Netzwerk-PBA-Einstellungen im DOC	74
2.3	Einstellungen für die Notfall-Anmeldung	75
2.4	DriveLock Agent	78
2.4.1	Installation der DriveLock-PBA auf dem DriveLock Agenten	78
2.4.2	Anmeldung an der DriveLock-PBA	79
2.4.3	Netzwerk-Preboot-Authentifizierung	82
2.4.4	Notfall-Anmeldung mit Wiederherstellungscode	84
2.5	DriveLock-PBA-Kommandozeilenprogramm	87
2.6	Abkürzungs- und Funktionstasten	89
3	DRIVELOCK BITLOCKER TO GO	92
3.1	Voraussetzungen für BitLocker To Go	92
3.2	Richtlinienkonfiguration von BitLocker To Go	93
3.2.1	Allgemeine Einstellungen für BitLocker To Go	94
3.2.2	Wiederherstellung verschlüsselter Laufwerke	95
3.2.2.1	Administrator-Kennwort	95
3.2.2.2	Zertifikatsbasierte Laufwerks-Wiederherstellung	96
3.2.3	Erzwungene Verschlüsselung	96
3.3	Beispielkonfiguration für eine Verschlüsselung mit BitLocker To Go	97
3.3.1	Laufwerks-Whitelist-Regel anlegen	99
3.4	BitLocker To Go-Wiederherstellung	101
3.4.1	Wiederherstellungsprozess	102
3.4.2	Wiederherstellung im DriveLock Operations Center (DOC)	103
3.5	DriveLock Agent	104

3.5.1 BitLocker To Go auf dem DriveLock Agenten	104
3.6 Verschiedene Anwendungsfälle	106
3.6.1 Administrator-Kennwort-Regeln	107
3.6.2 Verschlüsselungs-Regeln	108
INDEX	109
COPYRIGHT	111

1 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
- DriveLock BitLocker Management unterstützt neben den gängigen BitLocker Authentifizierungsmethoden auch Smartcard und Token.
- Sie können im DriveLock Control Center den Ver- und Entschlüsselungsstatus einzelner Geräte überwachen
- DriveLock BitLocker Management ermöglicht eine sichere und zentrale Verwaltung der BitLocker-Wiederherstellungsschlüssel
- Bei Verlust oder Diebstahl von Geräten kann eine Stilllegung bei erneuter Netzwerkverbindung schnell durchgeführt werden
- DriveLock BitLocker Management 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.

1.1 Allgemeines

1.1.1 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

- 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

- 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

- UEFI-Firmware erforderlich
- 64-Bit Betriebssysteme

- nur Professional, Enterprise und Education Edition
- kein TPM erforderlich (für höhere Sicherheit aber empfohlen)

1.1.2 Algorithmen für DriveLock BitLocker Management

Zur Festplattenverschlüsselung verwendet DriveLock 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	<ul style="list-style-type: none">• AES 128-bit mit Diffuser• AES 256-bit mit Diffuser• AES 128-bit• AES 256-bit
Windows 8.1	<ul style="list-style-type: none">• AES 128-bit• AES 256-bit
Windows 10	<ul style="list-style-type: none">• 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.

1.1.3 BitLocker Management lizenzieren

Um DriveLock BitLocker Management zu lizenzieren, Gehen Sie folgendermaßen vor::

1. Wählen Sie die Richtlinie aus, in der Sie DriveLock BitLocker Management lizenzieren wollen.
2. Gehen Sie unter **Globale Einstellungen** zu den **Einstellungen** und wählen dann **Lizenz** aus.
3. Öffnen Sie über das Kontextmenü die Lizenzeigenschaften und hier den Reiter **Lizenzen**.
4. Klicken Sie die Schaltfläche **Lizenzdatei hinzufügen...** und folgen Sie den Anweisungen auf dem Bildschirm.
5. Wählen Sie als nächstes Ihre **Lizenzdatei** aus (BitLocker Lizenz).



Hinweis: Wenn Sie die separate Lizenz für **DriveLock PBA for BitLocker** erworben haben, können Sie diese ebenfalls an dieser Stelle lizenzieren. Siehe auch [DriveLock PBA lizenzieren](#).

6. Im nächsten Dialog geben Sie an, wie Sie Ihre Lizenzdatei aktivieren möchten. Wir empfehlen die Online-Aktivierung.



Hinweis: Bei der Online-Aktivierung ist eine Verbindung zum Internet erforderlich.

7. Abschließend bestätigen Sie, dass Ihre Lizenz für DriveLock BitLocker Management dem DriveLock Enterprise Service hinzugefügt wird.
8. Im letzten Dialog bestätigen Sie ihre Einstellungen und aktivieren so die Verwendung von DriveLock BitLocker Management.
9. Unter den Lizenzeigenschaften im Reiter **Allgemein** wird nun Ihre Lizenz angezeigt.
10. Öffnen Sie als nächstes den Reiter **Lizenzierte Computer**. Wählen Sie **Alle Computer** aus, auf denen Sie DriveLock BitLocker Management verwenden wollen. Gegebenenfalls fügen Sie weitere Computer, Gruppen oder Organisationseinheiten hinzu, indem Sie die Schaltfläche **Hinzufügen** klicken.
11. Setzen Sie ein Häkchen bei DriveLock BitLocker Management.



Achtung: Sollten Sie bereits Disk Protection (DriveLock FDE) lizenziert haben, kann DriveLock BitLocker Management nicht gleichzeitig in derselben Richtlinie verwendet werden!

12. Klicken Sie **Bestätigen**, um Ihre Eingaben zu übernehmen und schließen Sie den Dialog mit **OK**.

1.2 Richtlinienkonfiguration von BitLocker

1.2.1 Verschlüsselungseinstellungen

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

Sobald Sie DriveLock BitLocker Management lizenziert, die Richtlinie gespeichert und neu geöffnet haben, wird in der entsprechenden Richtlinie im Knoten **Verschlüsselung** der neue Unterknoten DriveLock 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.

Einstellung	Wert
Verschlüsselungszertifikate	Zertifikate erzeugt am: Nie
Benutzerbezogene Agenteneinstellungen	Nicht konfiguriert
Einstellungen für die Pre-Boot-Authentifizierung	Nicht konfiguriert
Einstellungen für die Verschlüsselung	Nicht konfiguriert
Änderungen der lokalen PBA-Konfiguration zulassen	Nicht konfiguriert (Aktiviert)
SmartCard-Treiber in PBA laden	Nicht konfiguriert (Deaktiviert)
PBA-Tastatortreiber auswählen	Nicht konfiguriert (Standard UEFI-...)

1.2.1.1 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 Wiederherstellungsschlüssels und für eine eventuelle Notfall-Anmeldung).

DriveLock fügt die Verschlüsselungszertifikate automatisch in den Windows Zertifikatsspeicher ein, in dem auch die Kennwörter gespeichert werden.

 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 **DLBIDataRecovery.cer**) und dem privaten Schlüssel (in der Abbildung **DLBIDataRecovery.pfx**):

 DLBIDataRecovery.cer	04.12.2018 ...	Security Certificate
 DLBIDataRecovery.pfx	04.12.2018 ...	Personal Information Exchange

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

 DLBIEmergencyLogon.cer	04.12.2018 ...	Security Certificate
 DLBIEmergencyLogon.pfx	04.12.2018 ...	Personal Information Exchange

 **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.

1.2.1.1 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 DriveLock 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.

 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.

Verschlüsselungszertifikate erzeugen ×

Schutz für die Zertifikate 

Geben Sie die Kennwörter an, mit denen die privaten Schlüssel der Zertifikate geschützt werden.

 Private Schlüssel der Zertifikate werden per Kennwort geschützt. Diese Kennwörter werden nicht in der DriveLock-Richtlinie gespeichert, aber für eine Notfall-Anmeldung bzw. Wiederherstellung benötigt.
Bitte legen Sie diese Kennwörter an einer sicheren Stelle ab.

Kennwort für Notfall-Anmeldungszertifikat _____

Kennwort

Wiederholung

Kennwort für Wiederherstellungszertifikat _____

Kennwort

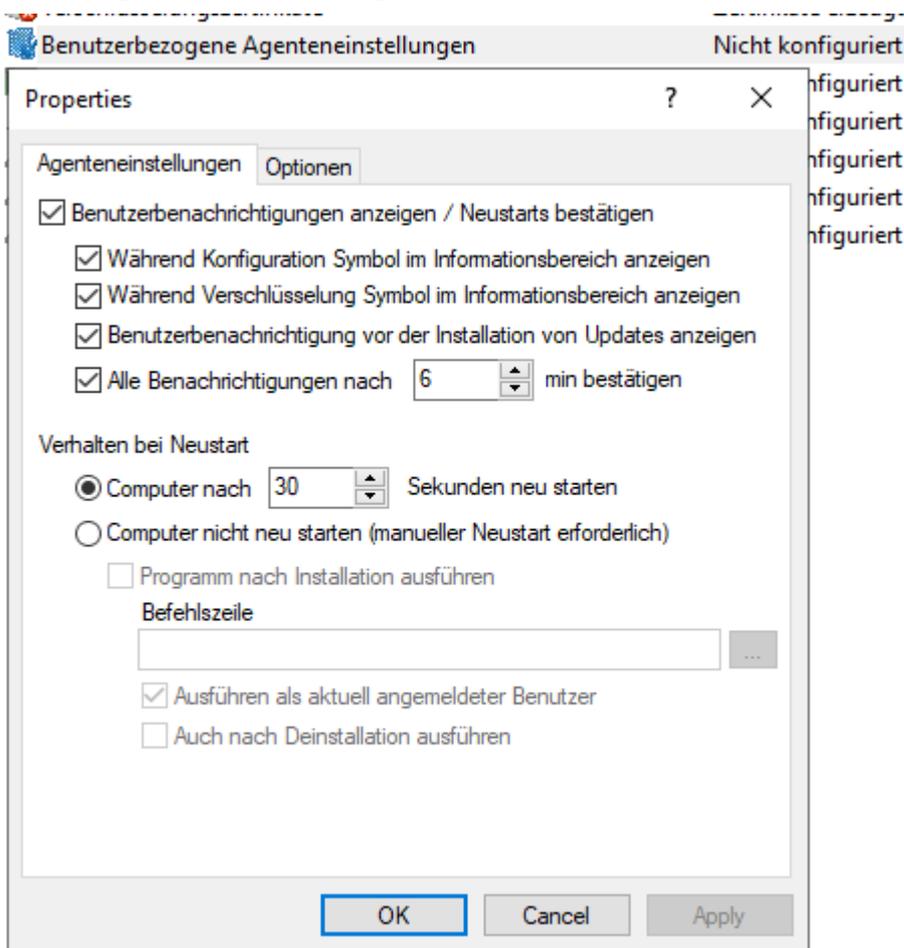
Wiederholung

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

1.2.1.2 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 Installationskript 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.

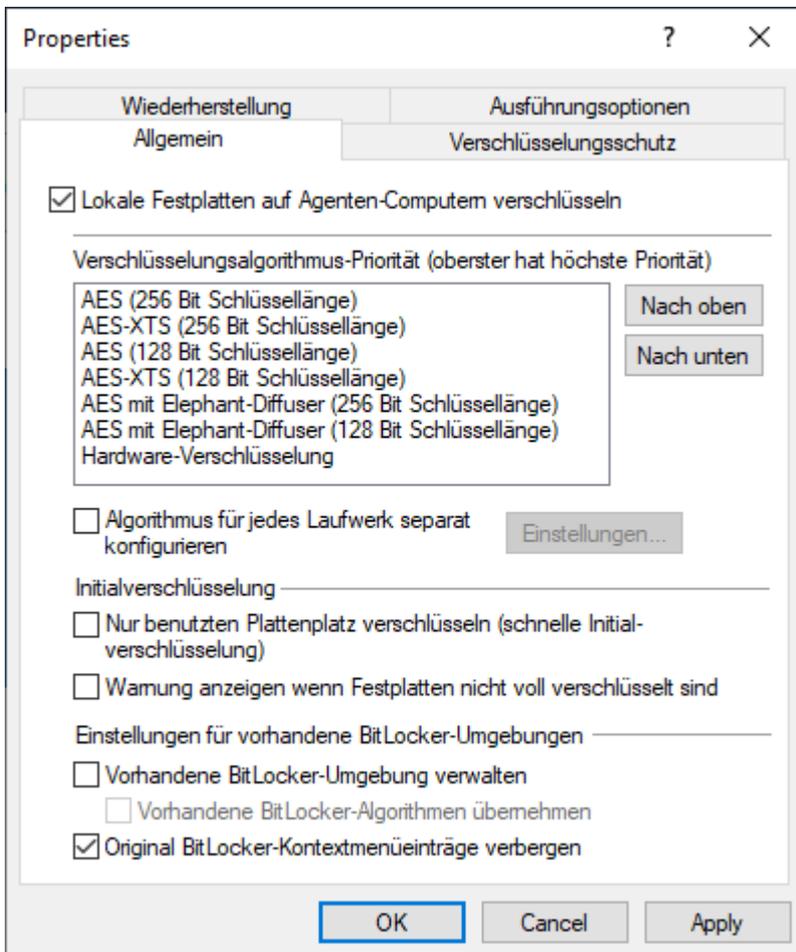
Auf dem Client-Computer erscheint dann eine Nachricht mit detaillierten Informationen (siehe Abbildung):



1.2.1.3 Einstellungen für die Verschlüsselung

1.2.1.3.1 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.

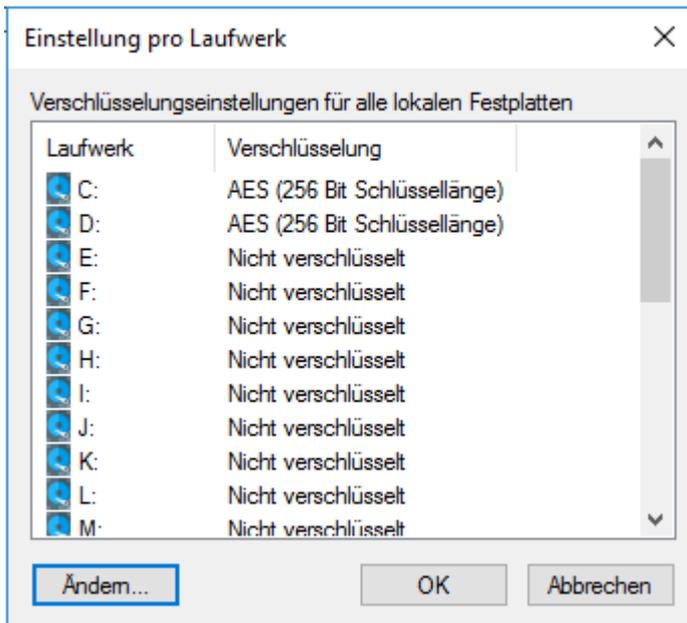
 **Hinweis:** Der stärkste Algorithmus sollte immer an oberster Stelle stehen.

- 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 Datenträger 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.

1.2.1.3.2 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:**

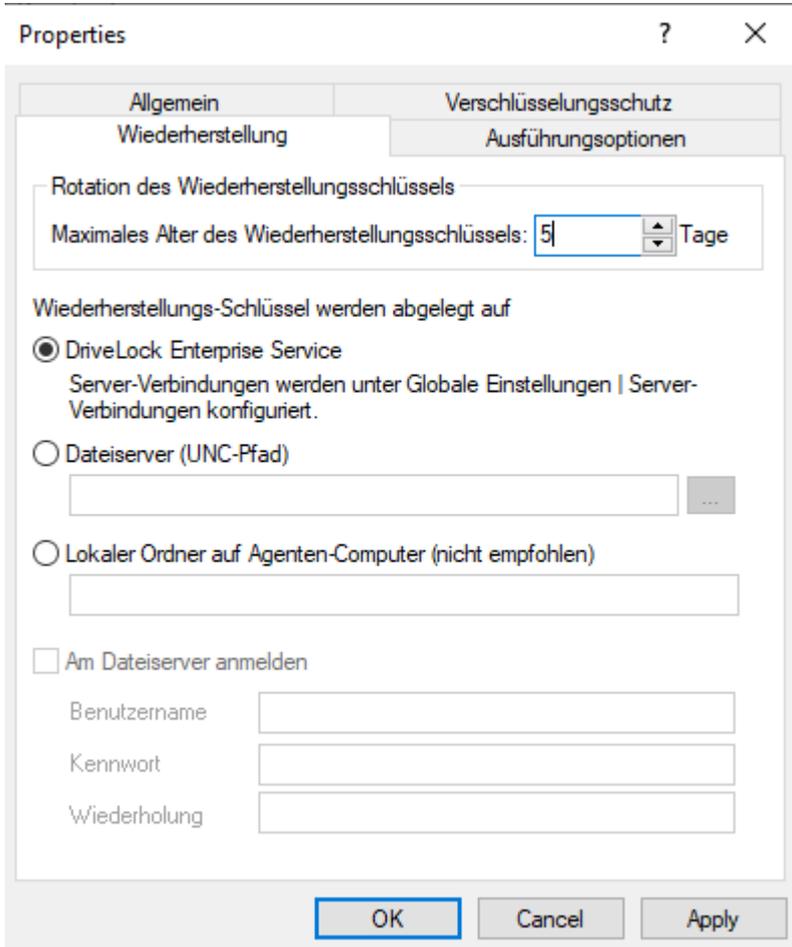
Diese Option ist standardmäßig aktiviert. Sie führt dazu, dass es zu keiner ungewollten Entschlüsselung der BitLocker Verschlüsselung kommt, wenn Konfigurationsänderungen durchgeführt werden, z.B. bei Aktualisierung des DriveLock Agenten, bei Änderungen von Gruppenmitgliedschaften oder wenn die Richtlinie 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.

1.2.1.3.3 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.

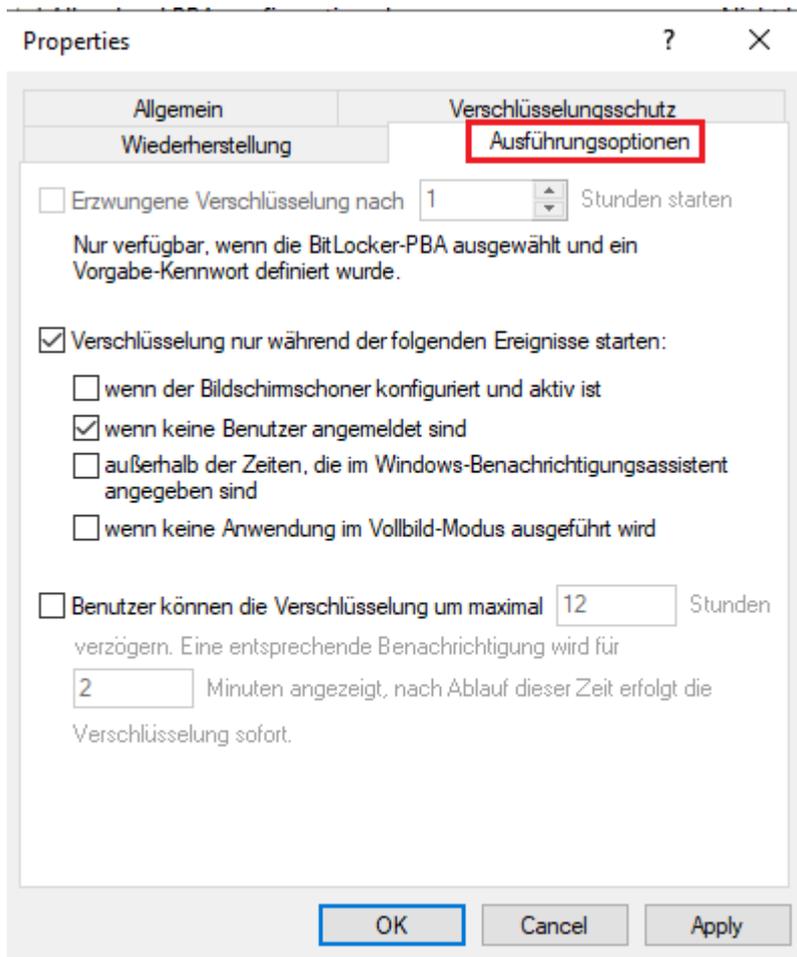
1.2.1.3.4 Reiter Ausführungsoptionen

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 Passwort (oder den PIN bei TPM) angeben.

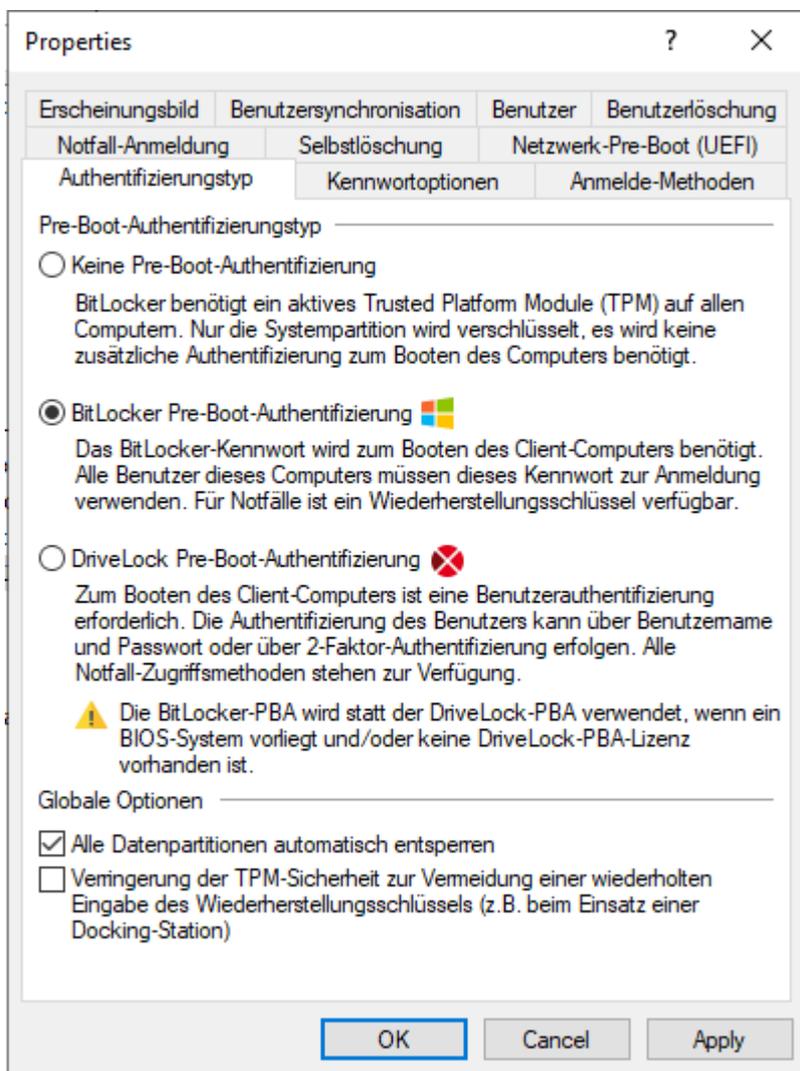
1.2.1.4 Einstellungen für die Pre-Boot-Authentifizierung

1.2.1.4.1 Reiter 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-Protector** 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, dass 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.

1.2.1.4.2 Reiter Kennwortoptionen

Auf diesem Reiter haben Sie verschiedene Möglichkeiten:

The screenshot shows the 'Properties' dialog box for BitLocker Pre-Boot Authentication, specifically the 'Kennwortoptionen' (Password Options) tab. The dialog is titled 'Properties' and has a question mark and a close button in the top right corner. The tabs at the top are: Erscheinungsbild, Benutzersynchronisation, Benutzer, Benutzerlöschung, Notfall-Anmeldung, Selbstlöschung, Netzwerk-Pre-Boot (UEFI), Authentifizierungstyp, Kennwortoptionen, and Anmelde-Methoden. The 'Kennwortoptionen' tab is selected. Below the tabs, it says 'Gültig für: BitLocker Pre-Boot-Authentifizierung'. There are two text input fields for 'Kennwort' and 'Bestätigen'. Below these are several checkboxes: 'Benutzer kann das Kennwort nicht ändern' (unchecked), 'Benutzer muss das Kennwort bei erstmaliger Verschlüsselung ändern' (checked), and 'Benutzerbezogene Wiederherstellungsinformationen sichern' (unchecked). The 'Maximales Kennwort-Alter' is set to 5 days. A warning icon indicates that encryption starts only when a password is entered. Below this, there are more checkboxes for password requirements: 'Kennwort muss den folgenden Voraussetzungen entsprechen:' (checked), 'Nur Zahlen erlauben' (unchecked), 'Zahlen und lateinische Buchstaben erlauben' (unchecked), 'Mindestlänge für Kennwörter' is 8 Zeichen, and 'Ein gültiges Kennwort muss mindestens enthalten...' with requirements for 1 Kleinbuchstaben, 1 Ziffer, 1 Großbuchstaben, and 1 Sonderzeichen. There is also an unchecked checkbox for 'Ziffern als Sonderzeichen behandeln'. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

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 Passwortlänge 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.

1.2.1.5 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 Tastatortreiber 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.

1.2.1.6 PBA-Tastatortreiber auswählen

Mit dieser Einstellung können Sie den Tastatortreiber 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-Tastatortreiber verwenden.

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

1.2.1.7 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.

1.2.2 Entschlüsselung

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

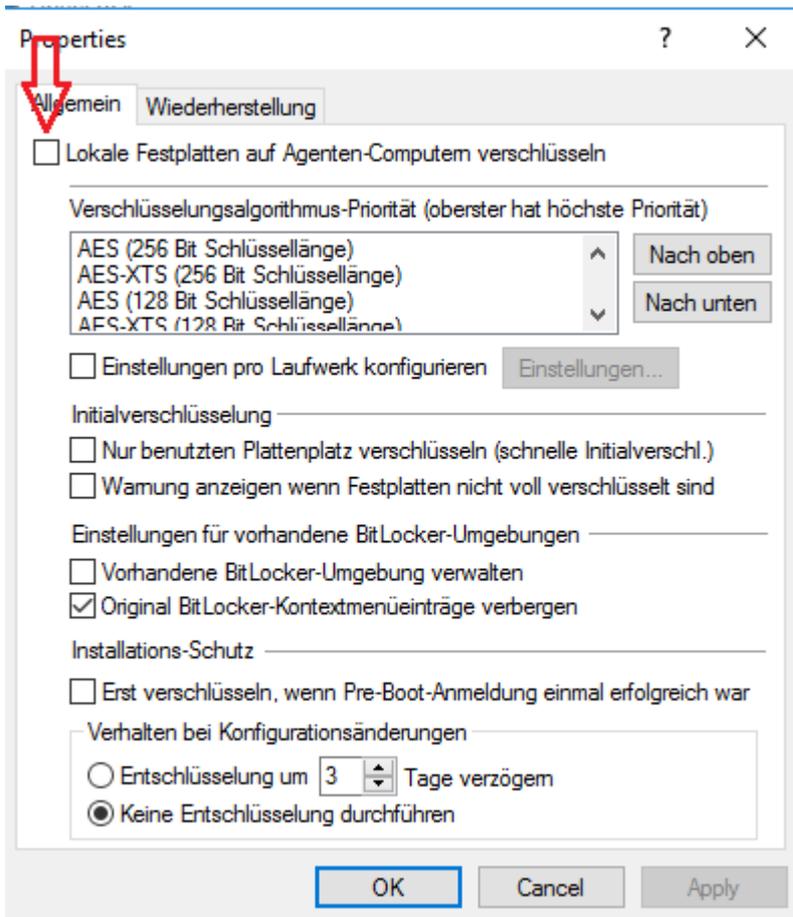
Der Entschlüsselungsprozess lässt sich, ebenso wie der Verschlüsselungsprozess, auch im DriveLock Operations Center (DoC) nachverfolgen.

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

1.2.2.1 Verschlüsselte Festplatten entschlüsseln

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

1. Öffnen Sie die entsprechende BitLocker-Richtlinie.
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**.



- Setzen Sie 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.

- 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.
- Bestätigen Sie Ihre Einstellungen mit **OK**.
- Auf dem Computer, dessen Festplatte entschlüsselt wird, erscheint nun folgende Meldung in der Statusleiste:



1.2.3 Richtlinie überschreiben (BitLocker)

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

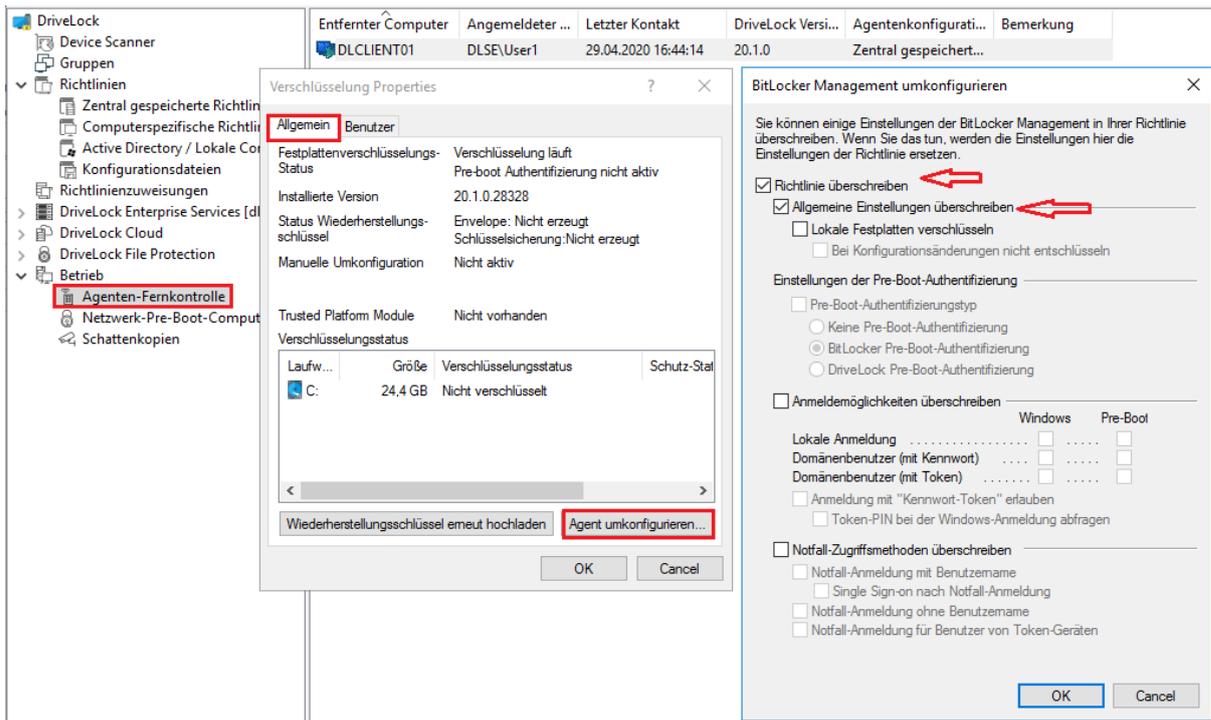
 **Achtung:** Beachten Sie bitte, dass die Richtlinieneinstellungen erst dann wieder aktiv werden, wenn Sie die Umkonfiguration wieder rückgängig gemacht haben.

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.

1.3 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 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 Entschlüsselungsverzögerung 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 im DriveLock Installations- und Administrationshandbuch unter <https://drivelock.help/>.

1.4 Wiederherstellung

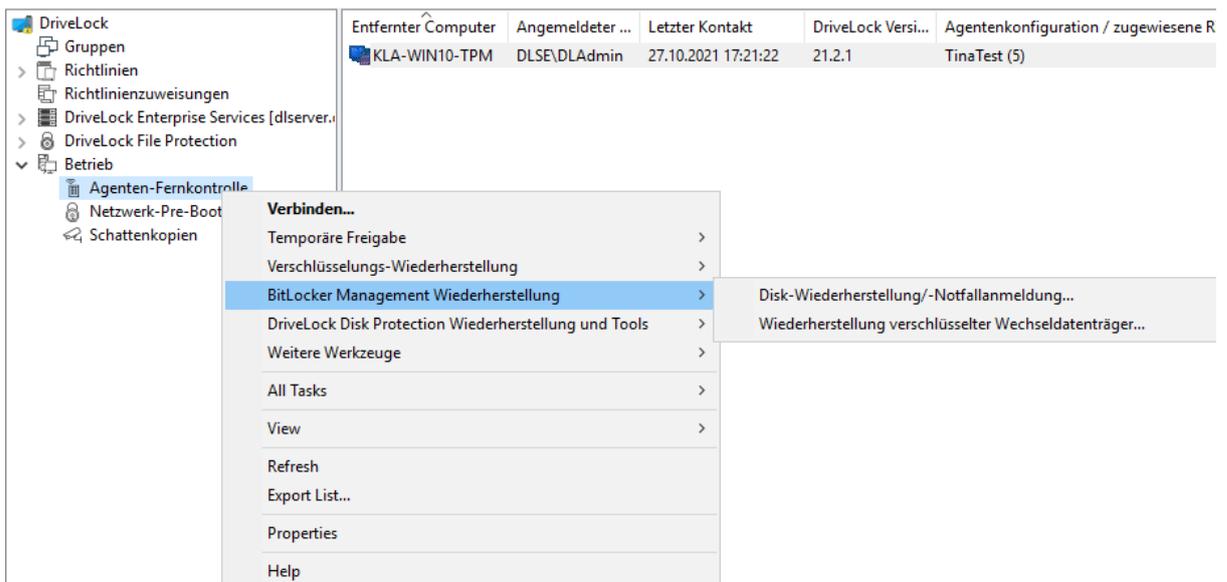
1.4.1 Wiederherstellung verschlüsselter Festplatten

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. Wählen Sie im **DriveLock Operations Center** den entsprechende Rechner über die Ansicht **Computer** aus. Öffnen Sie das Kontextmenü und wählen das Untermenü **BitLocker** und dann **Wiederherstellungsschlüssel anzeigen**. Geben Sie die Informationen zum Zertifikat bzw. zur Zertifikatsdatei und das zugehörige Kennwort ein.
2. Wählen Sie in der **DriveLock Management Konsole** den Knoten **Betrieb**, öffnen Sie das Kontextmenü der **Agenten-Fernkontrolle** und wählen dann den Menüpunkt **BitLocker Wiederherstellung** (s. Abbildung).

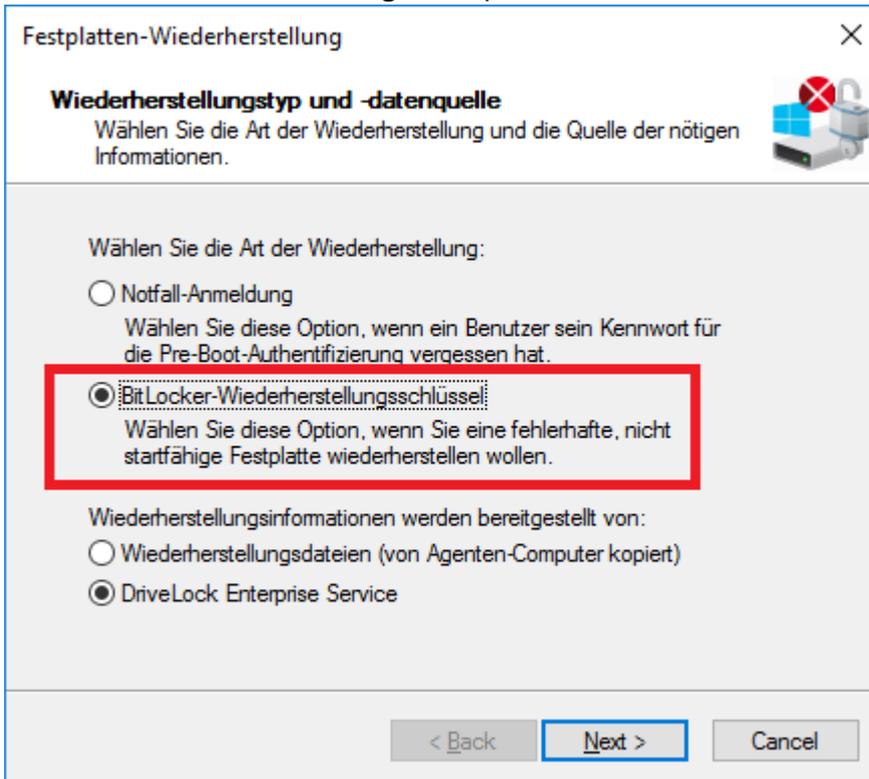


Hier öffnet sich der [Wiederherstellungsassistent](#), der Sie durch die jeweiligen Schritte führt.

1.4.2 Vorgehensweise zur Wiederherstellung

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.

The screenshot shows a Windows dialog box titled 'Festplatten-Wiederherstellung' (Hard Drive Recovery) with a close button (X) in the top right corner. The main heading is 'Private Schlüssel der Zertifikate' (Private Keys of Certificates) with a sub-instruction: 'Wählen Sie den benötigten privaten Schlüssel und sein Kennwort.' (Select the required private key and its password). To the right of the heading is an icon of a padlock with a red 'X' over it. Below the heading, there is explanatory text: 'Verschlüsselungszertifikate und deren private Schlüssel werden für die Wiederherstellung benötigt. Geben Sie den Speicherort der Zertifikate und privaten Schlüssel an.' (Encryption certificates and their private keys are required for recovery. Specify the location of the certificates and private keys). Three radio buttons are present: 'Windows-Zertifikatsspeicher' (Windows Certificate Store), 'Smart card', and 'Dateisystem (PFX-Dateien)' (File system (PFX files)), with the third one selected. Below these are two input fields: 'Datei des Datenwiederherstellungszertifikats (PFX)' (File of the data recovery certificate (PFX)) with a browse button (...), and 'Kennwort der PFX-Datei' (PFX file password). At the bottom, there are three buttons: '< Back' (highlighted in blue), 'Next >', and 'Cancel'.

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

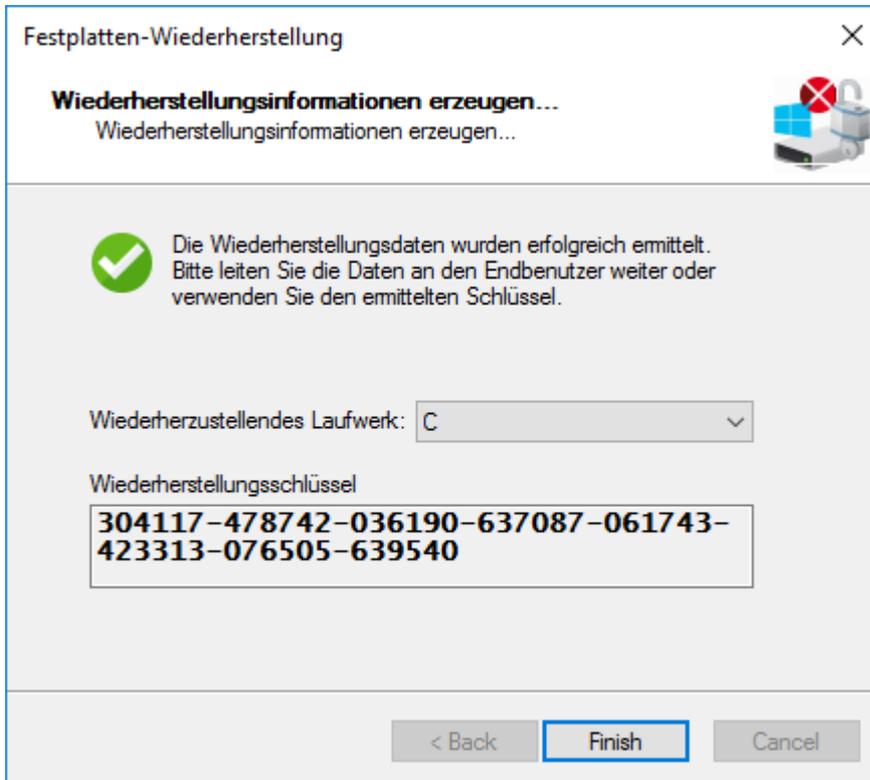
 Hinweis: Wenn Sie in den Einstellungen zur Verschlüsselung angegeben haben, dass die Wiederherstellungsinformationen im Dateisystem liegen, müssen Sie hier auch direkt das dazugehörige Kennwort für den privaten Schlüssel eingeben.

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.

 Hinweis: Das Challenge-Response-Verfahren steht erst in der nächsten Version vollständig zur Verfügung.

6. Warten Sie nun einen Moment ab, während die Wiederherstellungsinformationen ermittelt werden.
7. Der nächste Dialog zeigt Ihnen bereits den Wiederherstellungsschlüssel an.

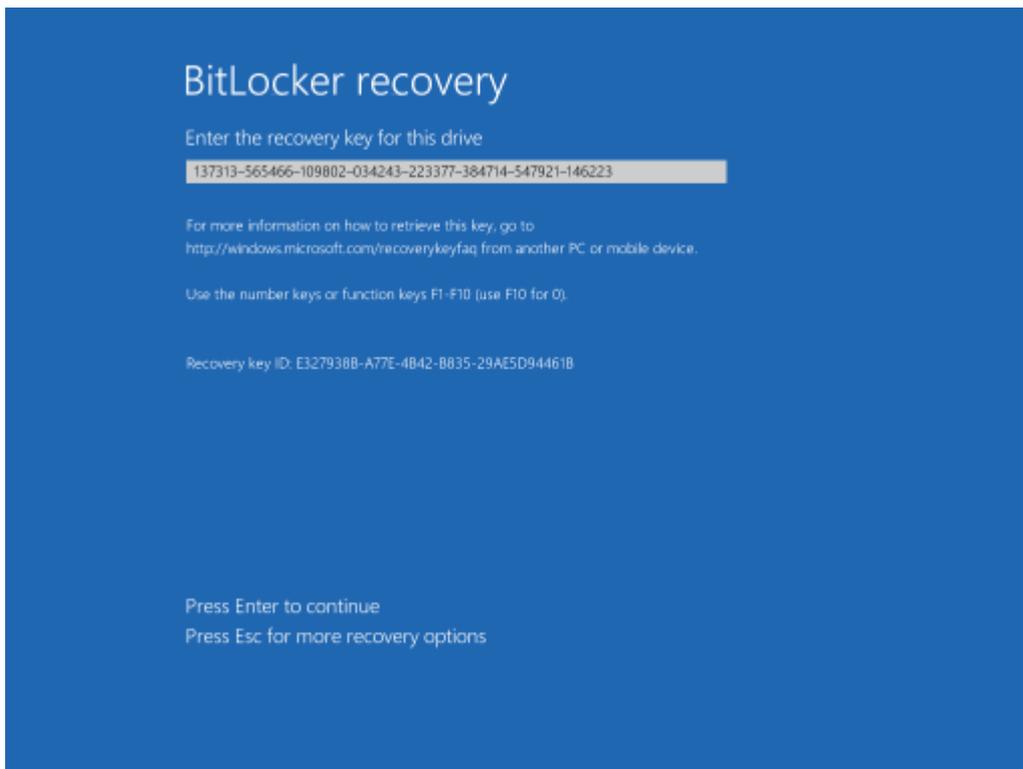
 Hinweis: Wählen Sie hier das Laufwerk aus, das als Systempartition auf dem Client-Computer definiert ist.



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 Wiederherstellungsschlüssel ein erhebliches Sicherheitsrisiko darstellt. Aus diesem Grund veranlasst DriveLock BitLocker Management eine benutzerseitige Kennwortänderung und tauscht den Wiederherstellungsschlüssel 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.

1.5 Übernahme

1.5.1 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.

1.5.2 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 eine 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.

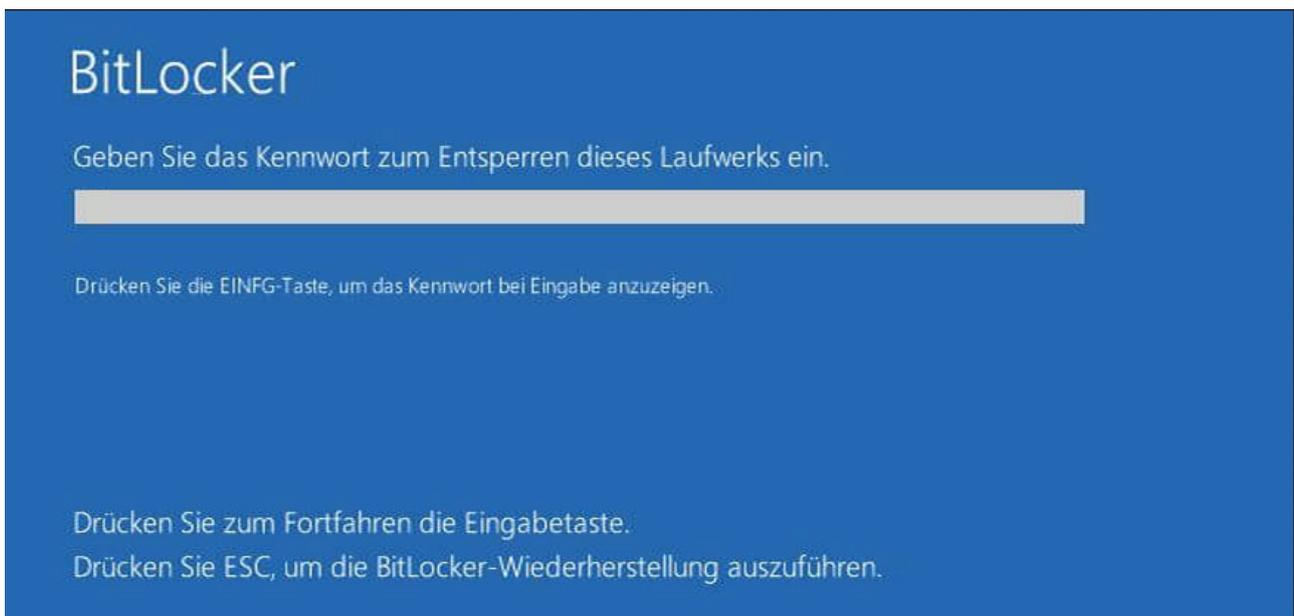
- wenn in den Lizenzoptionen unter **Lizenzierte Computer** die Option **Bitlocker Management** deaktiviert wird.
- **Verschlüsseln neu hinzugekommener Partitionen**
Eine Verschlüsselung sollte immer dann angestoßen werden, wenn neue Hardware hinzukommt oder ein Laufwerk hinzugefügt wird (in der Option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

1.6 DriveLock Agent

1.6.1 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 EING-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.

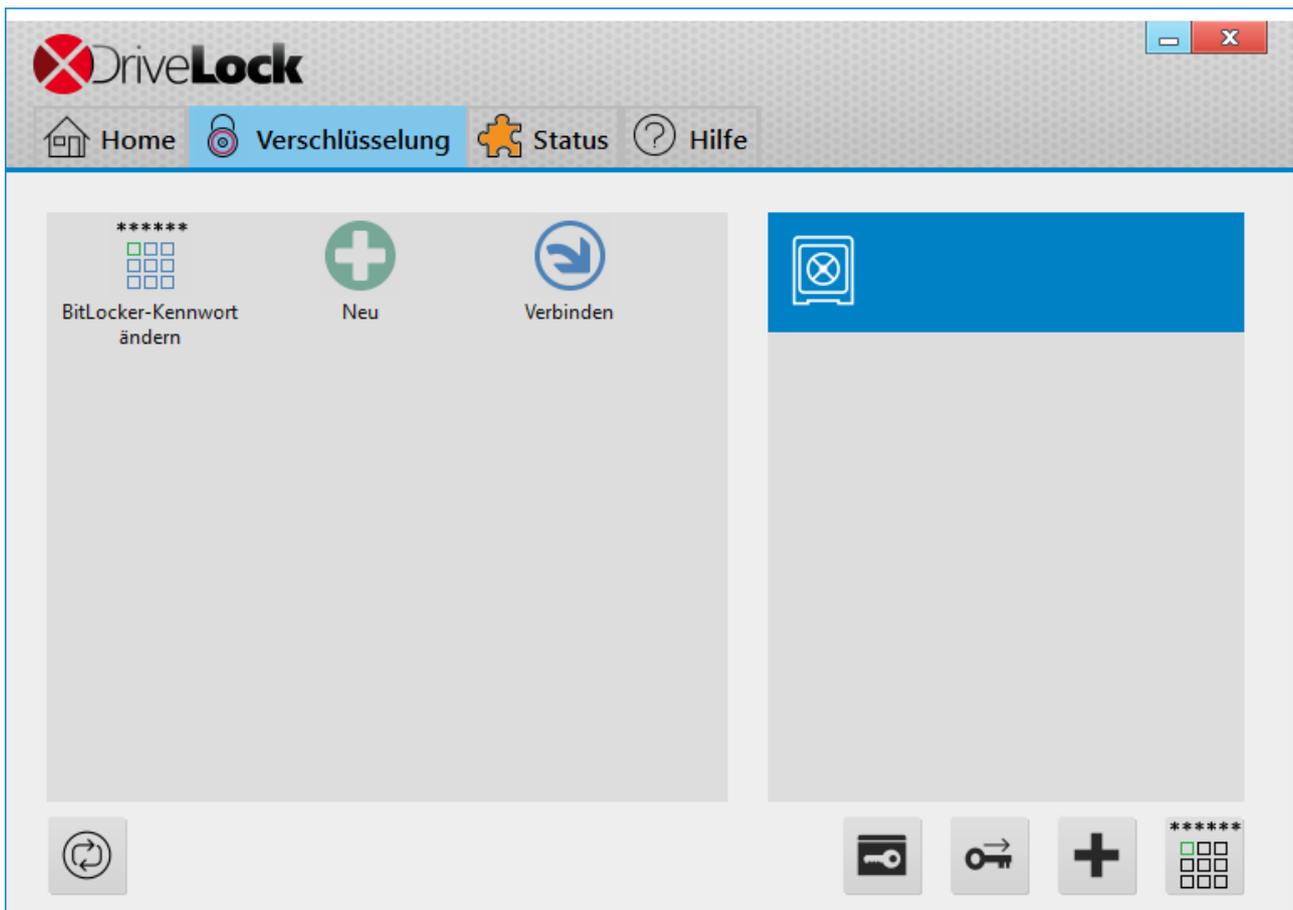


1.6.2 BitLocker Management auf Client-Computern (DriveLock Agent)

Mit der Zuweisung Ihrer BitLocker-Richtlinie 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.



1.6.3 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:

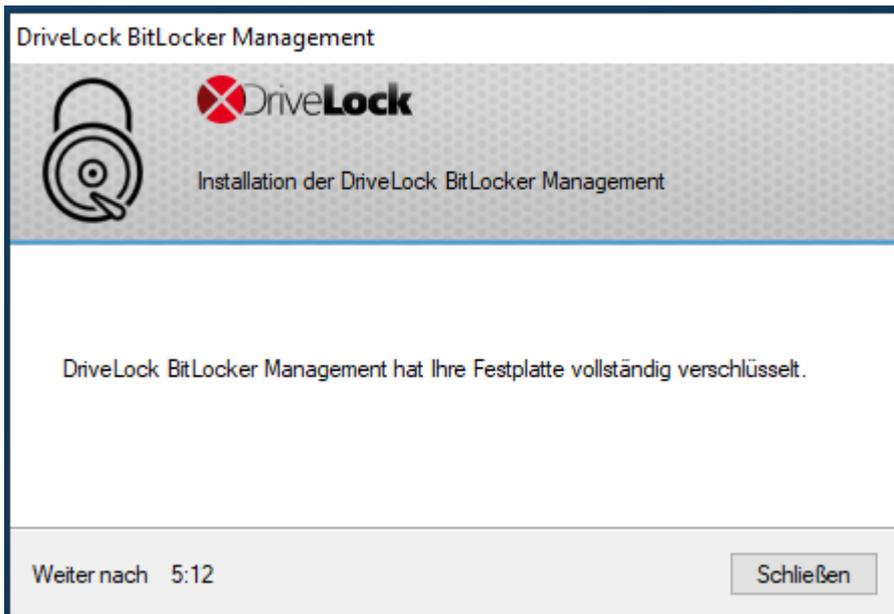


Nach Beenden der Verschlüsselung erscheint die in Punkt 5. beschriebene Meldung.

- 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.

1.6.3.1 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



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.

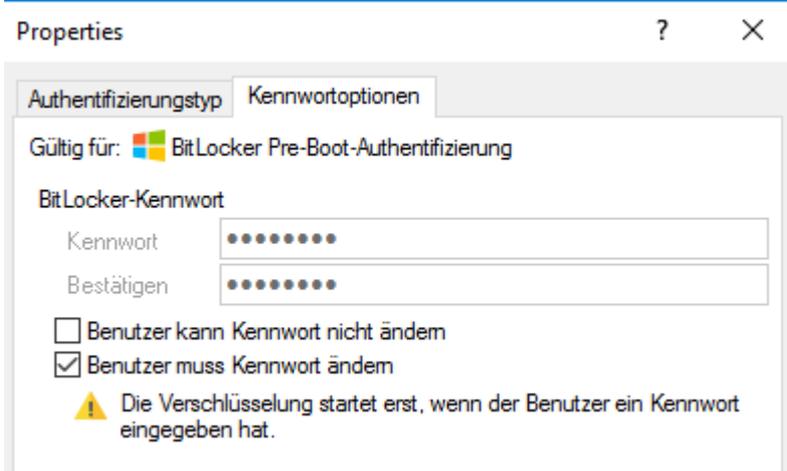
Um die Verschlüsselung sofort zu starten, klicken Sie die Schaltfläche Verschlüsseln.

Verschlüsselung
starten in 4:52 Verzögern um 10Min.

1.6.4 Datenpartition mit vorhandenem BitLocker übernehmen

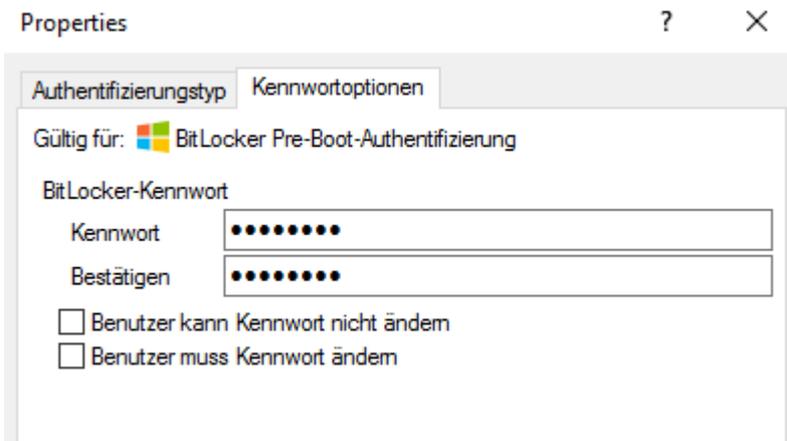
Das Vorgehen zum Entsperren von Datenpartitionen, die mit original BitLocker verschlüsselt wurden, und in DriveLock BitLocker Management übernommen werden sollen, richtet sich nach zwei Einstellungen in den **Kennwortoptionen** der BitLocker-Richtlinie:

- 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.

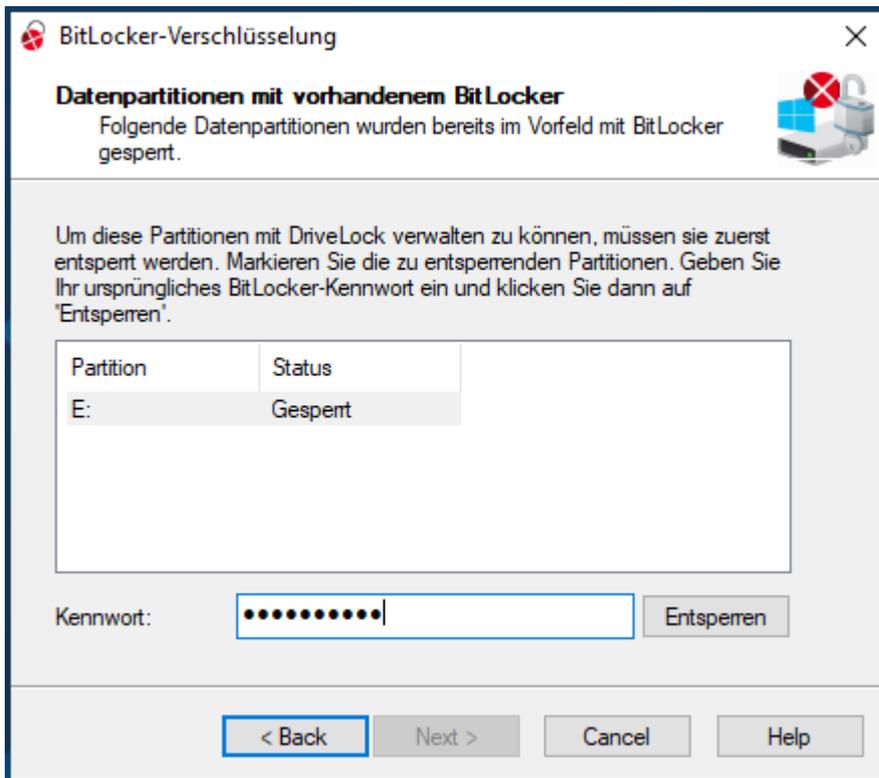


- Der andere Assistent enthält lediglich Information zur Übernahme der bestehenden BitLocker-Umgebung:



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

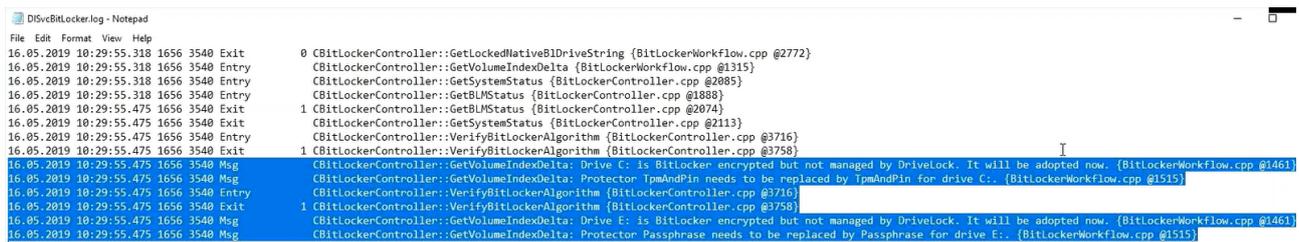
Den jeweiligen Abschlussdialog schließen Sie mit **Fertigstellen** ab.

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

1.7 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 `DLSvc-cBitLocker.log`, siehe Abbildung unten. Hier lässt sich genau ersehen, welche Aktionen DriveLock bei der Übernahme von bestehenden BitLocker-Umgebungen durchführt.



```

DLSvcBitLocker.log - Notepad
File Edit Format View Help
16.05.2019 10:29:55.318 1656 3540 Exit      0 CBitLockerController::GetLockedNativeBIDriveString {BitLockerWorkflow.cpp @2772}
16.05.2019 10:29:55.318 1656 3540 Entry    CBitLockerController::GetVolumeIndexDelta {BitLockerWorkflow.cpp @1315}
16.05.2019 10:29:55.318 1656 3540 Entry    CBitLockerController::GetSystemStatus {BitLockerController.cpp @2085}
16.05.2019 10:29:55.318 1656 3540 Entry    CBitLockerController::GetBLMStatus {BitLockerController.cpp @1888}
16.05.2019 10:29:55.475 1656 3540 Exit      1 CBitLockerController::GetBLMStatus {BitLockerController.cpp @2074}
16.05.2019 10:29:55.475 1656 3540 Exit    CBitLockerController::GetSystemStatus {BitLockerController.cpp @2113}
16.05.2019 10:29:55.475 1656 3540 Entry    CBitLockerController::VerifyBitLockerAlgorithm {BitLockerController.cpp @3716}
16.05.2019 10:29:55.475 1656 3540 Exit      1 CBitLockerController::VerifyBitLockerAlgorithm {BitLockerController.cpp @3758}
16.05.2019 10:29:55.475 1656 3540 Msg      CBitLockerController::GetVolumeIndexDelta: Drive C: is BitLocker encrypted but not managed by DriveLock. It will be adopted now. {BitLockerWorkflow.cpp @1461}
16.05.2019 10:29:55.475 1656 3540 Msg      CBitLockerController::GetVolumeIndexDelta: Protector TpmAndPin needs to be replaced by TpmAndPin for drive C:. {BitLockerWorkflow.cpp @1515}
16.05.2019 10:29:55.475 1656 3540 Entry    CBitLockerController::VerifyBitLockerAlgorithm {BitLockerController.cpp @3716}
16.05.2019 10:29:55.475 1656 3540 Exit      1 CBitLockerController::VerifyBitLockerAlgorithm {BitLockerController.cpp @3758}
16.05.2019 10:29:55.475 1656 3540 Msg      CBitLockerController::GetVolumeIndexDelta: Drive E: is BitLocker encrypted but not managed by DriveLock. It will be adopted now. {BitLockerWorkflow.cpp @1461}
16.05.2019 10:29:55.475 1656 3540 Msg      CBitLockerController::GetVolumeIndexDelta: Protector Passphrase needs to be replaced by Passphrase for drive E:. {BitLockerWorkflow.cpp @1515}

```

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.

2 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 in Windows 10 Umgebungen funktioniert.

Die ältere BIOS PBA kann lediglich in Windows 7 oder 8.1 Umgebungen verwendet werden, sie wird nicht mehr aktualisiert und dient nur noch für DriveLock Disk Protection (FDE). Wenn BitLocker Management auf BIOS-Systemen eingesetzt wird, wird die original BitLocker PBA verwendet.

 **Hinweis:** Informationen zum Einsatz der PBA mit DriveLock Disk Protection finden Sie im entsprechenden Kapitel des Admin Handbuchs unter Product Documentation auf der [DriveLock.Help](https://www.dell.com/support/learn/learn-to-go?lang=en) Website.

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

- Anmeldung mit Benutzername/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

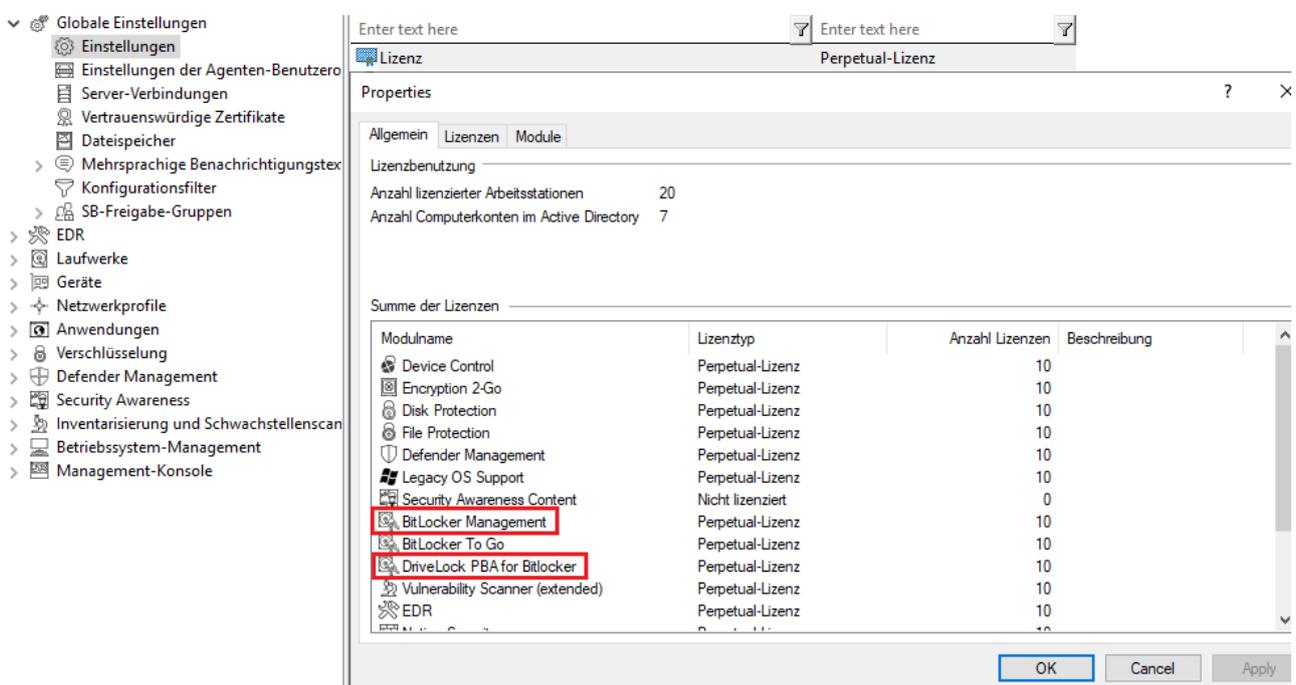
2.1 Richtlinienkonfiguration der Pre-Boot-Authentifizierung

Bitte beachten Sie, dass die DriveLock PBA für BitLocker Management eine separate Lizenz erfordert, die auf der BitLocker Management Lizenz aufbaut.

2.1.1 DriveLock PBA lizenzieren

Die Lizenzierung der **DriveLock PBA for BitLocker** erfolgt wie im Kapitel [BitLocker Management lizenzieren](#) beschrieben.

 Hinweis: Beachten Sie bitte, dass beide Lizenzen ausgewählt sind, wie in der Abbildung unten gezeigt.



The screenshot displays the 'Lizenz' (License) management window. The left sidebar shows the navigation tree with 'Einstellungen' (Settings) expanded to 'Verschlüsselung' (Encryption) and 'BitLocker Management' selected. The main window shows a table of licenses with the following data:

Modulname	Lizentyp	Anzahl Lizenzen	Beschreibung
Device Control	Perpetual-Lizenz	10	
Encryption 2-Go	Perpetual-Lizenz	10	
Disk Protection	Perpetual-Lizenz	10	
File Protection	Perpetual-Lizenz	10	
Defender Management	Perpetual-Lizenz	10	
Legacy OS Support	Perpetual-Lizenz	10	
Security Awareness Content	Nicht lizenziert	0	
BitLocker Management	Perpetual-Lizenz	10	
BitLocker To Go	Perpetual-Lizenz	10	
DriveLock PBA for Bitlocker	Perpetual-Lizenz	10	
Vulnerability Scanner (extended)	Perpetual-Lizenz	10	
EDR	Perpetual-Lizenz	10	

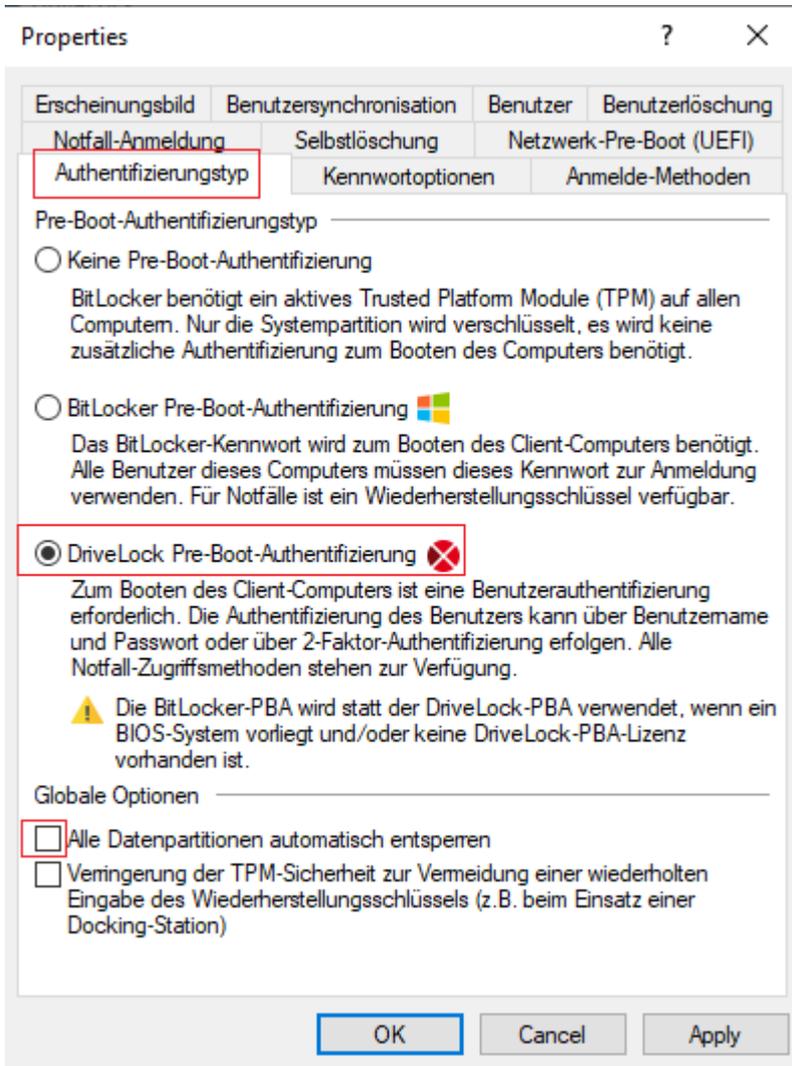
2.1.2 Einstellungen für die Pre-Boot-Authentifizierung

Um die DriveLock Pre-Boot Authentifizierung für BitLocker zu konfigurieren, wählen Sie als erstes im Knoten **Verschlüsselung** den Unterknoten **BitLocker Management** und dann **Festplattenverschlüsselung**. Beginnen Sie am besten mit der Einstellung des **Authentifizierungstyps**.

2.1.2.1 Authentifizierungstyp

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 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.

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

 Achtung: Nur wenn die Optionen Windows und Preboot 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.

2.1.2.3 Benutzer

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

BitLocker Management fügt jeden Benutzer zur Pre-Boot-Authentifizierungs-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 Schaltfläche **Hinzufügen** können Sie Benutzer manuell hinzufügen.

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.

2.1.2.4 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.

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.

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



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.

2.1.2.5 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.

2.1.2.6 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. Derzeit ist diese Option noch nicht für die DriveLock-PBA, sondern nur für DriveLock BitLocker Management verfügbar.
- Falls gewünscht, können Sie Ihren eigenen Anzeigetext im Textfeld unter der Option **Pre-Boot-Benutzerinformationen anzeigen** eingeben.

2.1.2.7 Netzwerk-Pre-Boot (UEFI)

Informationen zu diesem Reiter finden Sie [hier](#).

2.1.2.8 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 Passwort-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 Passwort vergessen haben - auch wenn ein Administrator das Passwort 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** vornehmen.

2.1.2.9 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.

2.1.3 Richtlinie überschreiben (DriveLock PBA)

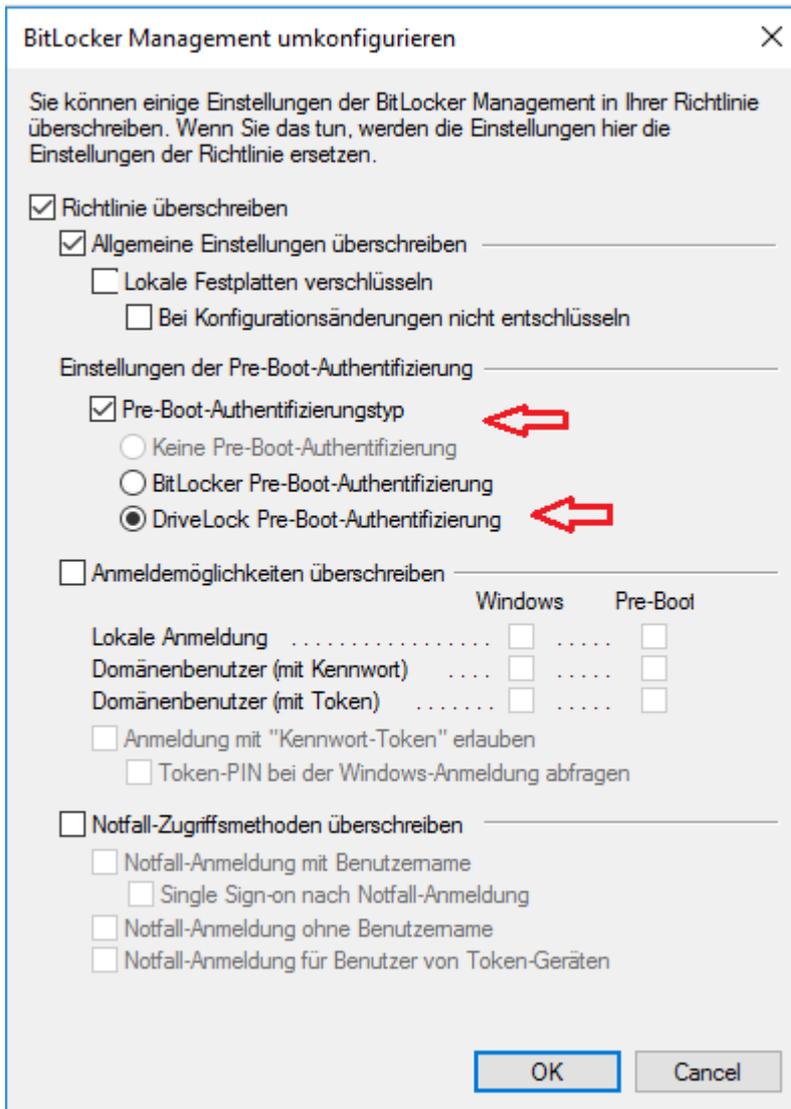
Um auf einzelnen Client-Computern gezielt Pre-Boot-Authentifizierungseinstellungen außer Kraft zu setzen, können Sie bereits gesetzte Richtlinieneinstellungen überschreiben.



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).



- 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).

- 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](#).
- Wenn Sie jetzt **OK** klicken, werden Ihre Einstellungen mit sofortiger Wirkung auf dem gewählten Client-Computer angewendet.

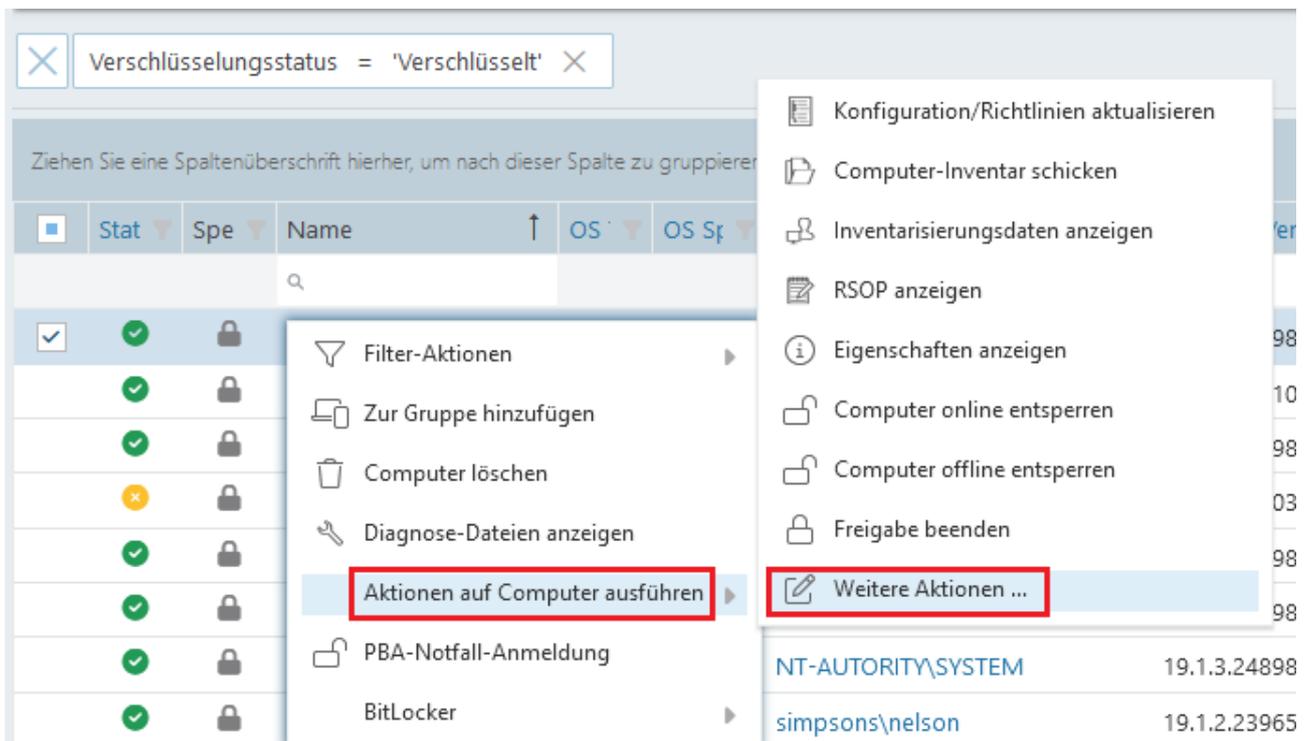
2.1.4 PBA-Einstellungen im DriveLock Operations Center (DOC)

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:

Pre-Boot-Authentifizierung (PBA)

PBA temporär deaktivieren

Im Zeitraum von



-



Für die eingestellte Anzahl von Neustarts

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.

2.2 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, die 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-Patches auf unbeaufsichtigte Client-Computer.

Beachten Sie folgende Einschränkungen:

- Es wird nur UEFI-Firmware unterstützt (nur beim Einsatz von DriveLock Disk Protection bleibt die Netzwerk-PBA für BIOS weiterhin funktionsfähig)
- 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
- 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.

2.2.1 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 ('AutoLogin-Benutzer') mit autogeneriertem Benutzerkennwort
- Austausch eines RSA-Schlüsselpaars 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](#).

- 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!

- 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.

- Anmeldung über das Active Directory (AD) erlauben:** Wählen Sie diese Option, um Anmeldeinformationen aus dem AD zu beziehen.
- 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](#).
- 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.
- Anzahl der automatischen Wiederholversuche bis zum Zustandekommen der Netzwerkverbindung:** Geben Sie hier an, wie oft das System automatisch versuchen

soll, eine Netzwerkverbindung herzustellen.

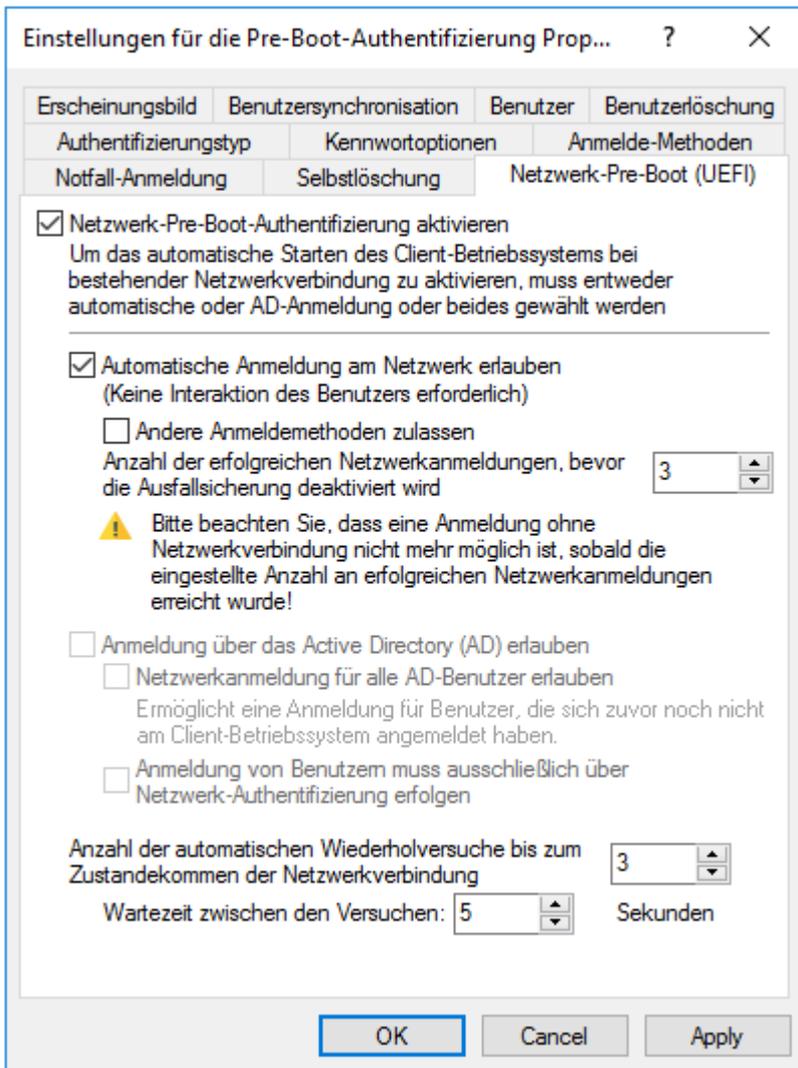
9. **Wartezeit zwischen den Versuchen:** Geben Sie hier die Sekunden an, die zwischen den Wiederholversuchen liegen darf. Standardwert ist 5 Sekunden.

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.

2.2.2 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 Anmeldeverfahren 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**.

2.2.3 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):

Einstellungen für die Pre-Boot-Authentifizierung Prop... ? X

Erscheinungsbild Benutzersynchronisation Benutzer Benutzerlöschung

Authentifizierungstyp Kennwortoptionen Anmelde-Methoden

Notfall-Anmeldung Selbstlöschung Netzwerk-Pre-Boot (UEFI)

Netzwerk-Pre-Boot-Authentifizierung aktivieren
Um das automatische Starten des Client-Betriebssystems bei bestehender Netzwerkverbindung zu aktivieren, muss entweder automatische oder AD-Anmeldung oder beides gewählt werden

Automatische Anmeldung am Netzwerk erlauben
(Keine Interaktion des Benutzers erforderlich)

Andere Anmeldeverfahren zulassen
Anzahl der erfolgreichen Netzwerkanmeldungen, bevor die Ausfallsicherung deaktiviert wird 3

Anmeldung über das Active Directory (AD) erlauben

Netzwerkanmeldung für alle AD-Benutzer erlauben
Ermöglicht eine Anmeldung für Benutzer, die sich zuvor noch nicht am Client-Betriebssystem angemeldet haben.

Anmeldung von Benutzern muss ausschließlich über Netzwerk-Authentifizierung erfolgen

Anzahl der automatischen Wiederholversuche bis zum Zustandekommen der Netzwerkverbindung 3

Wartezeit zwischen den Versuchen: 5 Sekunden

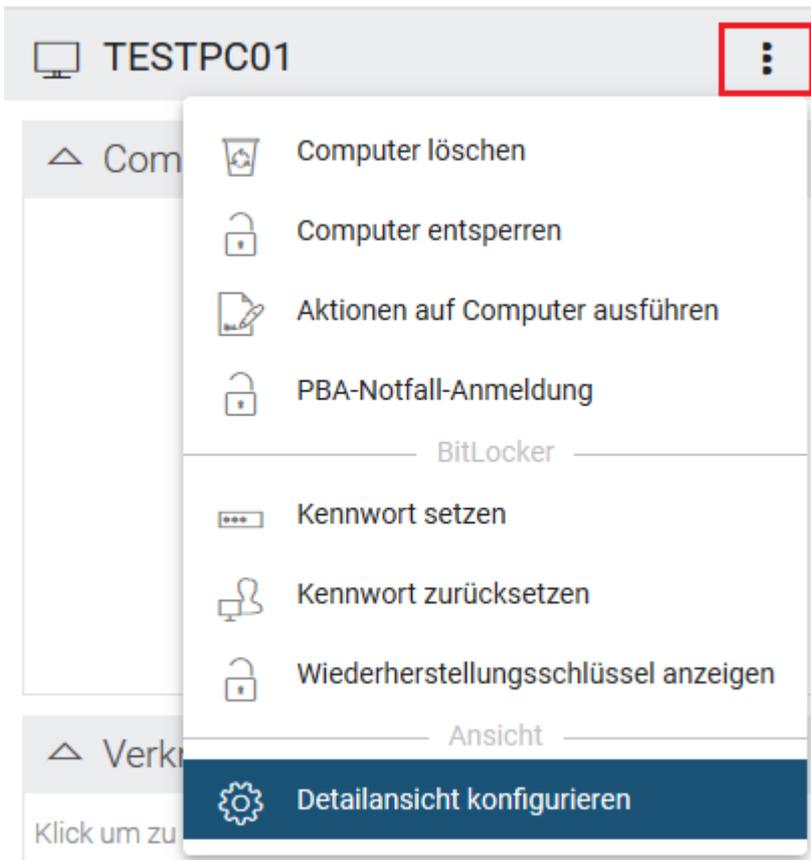
OK Cancel Apply

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**.

2.2.4 Netzwerk-PBA-Einstellungen im DOC

Gehen Sie folgendermaßen vor, um Einstellungen zur Netzwerk-Pre-Boot-Authentifizierung 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 Auswahlménü, 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.

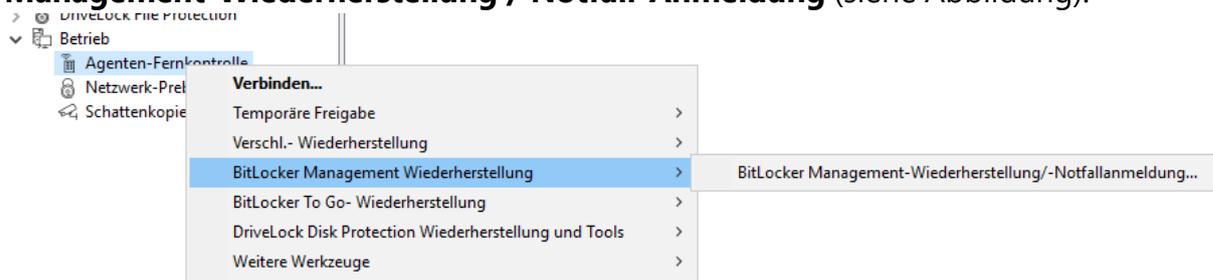
2.3 Einstellungen für die Notfall-Anmeldung

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.

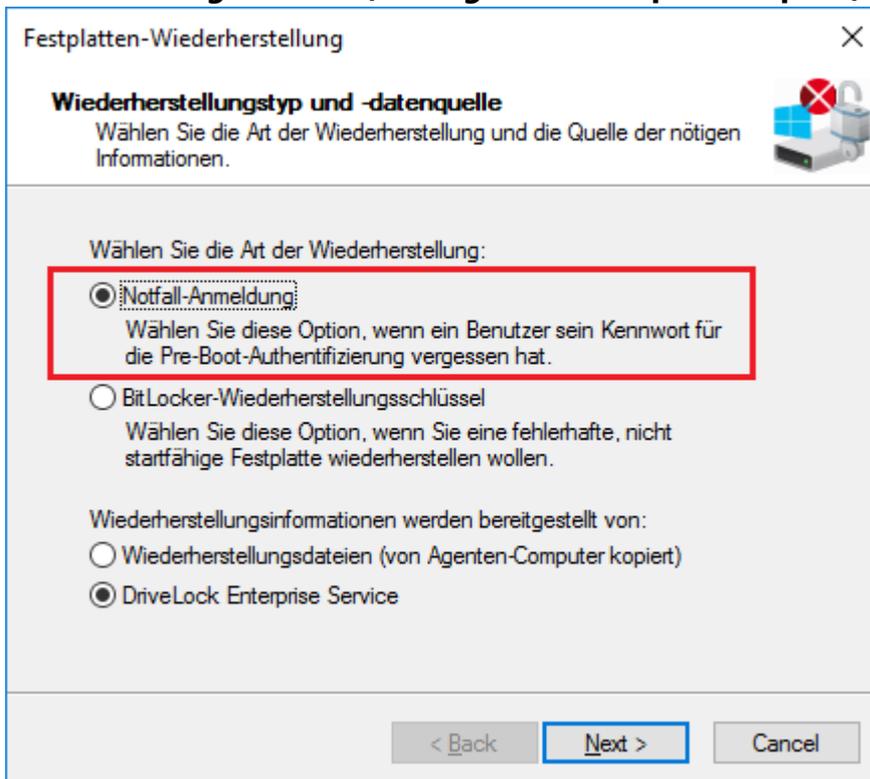
Gehen Sie folgendermaßen vor:

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).



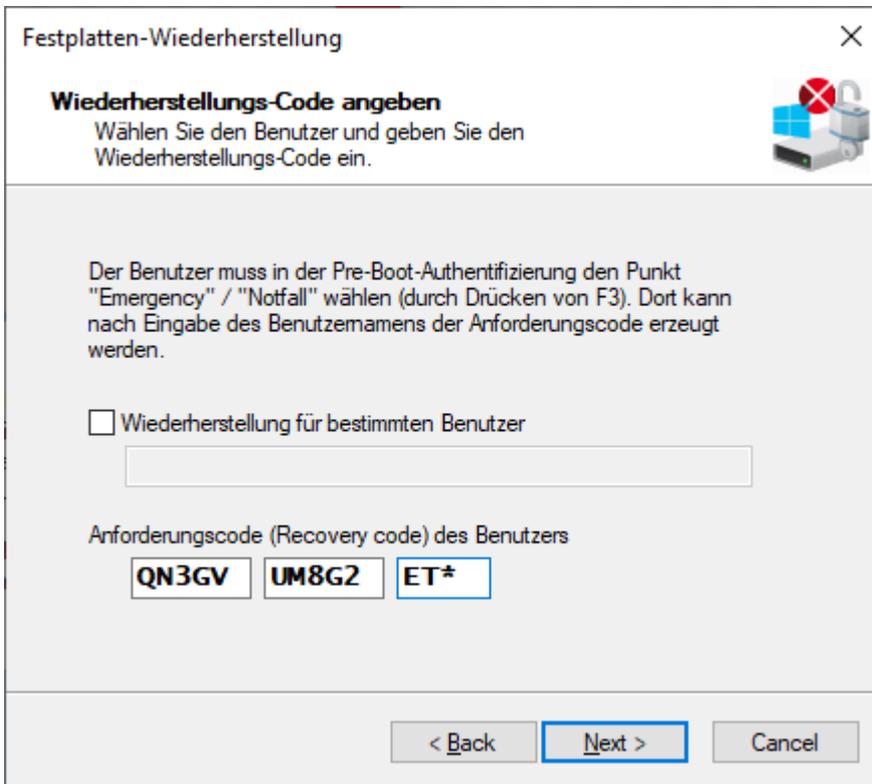
3. Der Wiederherstellungs-Assistent wird geöffnet. Wählen Sie auf der ersten Seite die Option **Notfall-Anmeldung**. Wenn Ihre Wiederherstellungs-Schlüssel zum DriveLock Enterprise Service gesendet werden, lassen Sie die Standardeinstellung **DriveLock Enterprise Service**. Wenn Sie den Pfad später zu 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. Wiederherstellungscode 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.



Festplatten-Wiederherstellung

Wiederherstellungs-Code angeben
Wählen Sie den Benutzer und geben Sie den Wiederherstellungs-Code ein.

Der Benutzer muss in der Pre-Boot-Authentifizierung den Punkt "Emergency" / "Notfall" wählen (durch Drücken von F3). Dort kann nach Eingabe des Benutzernamens der Anforderungscode erzeugt werden.

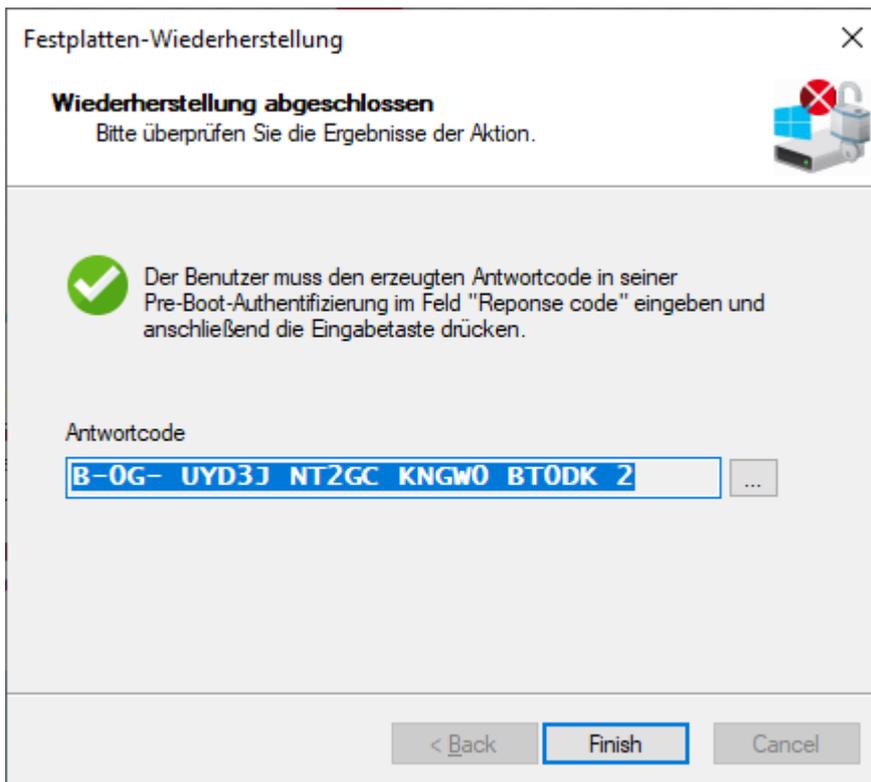
Wiederherstellung für bestimmten Benutzer

Anforderungscode (Recovery code) des Benutzers

QN3GV UM8G2 ET*

< Back Next > Cancel

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



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

2.4 DriveLock Agent

2.4.1 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.

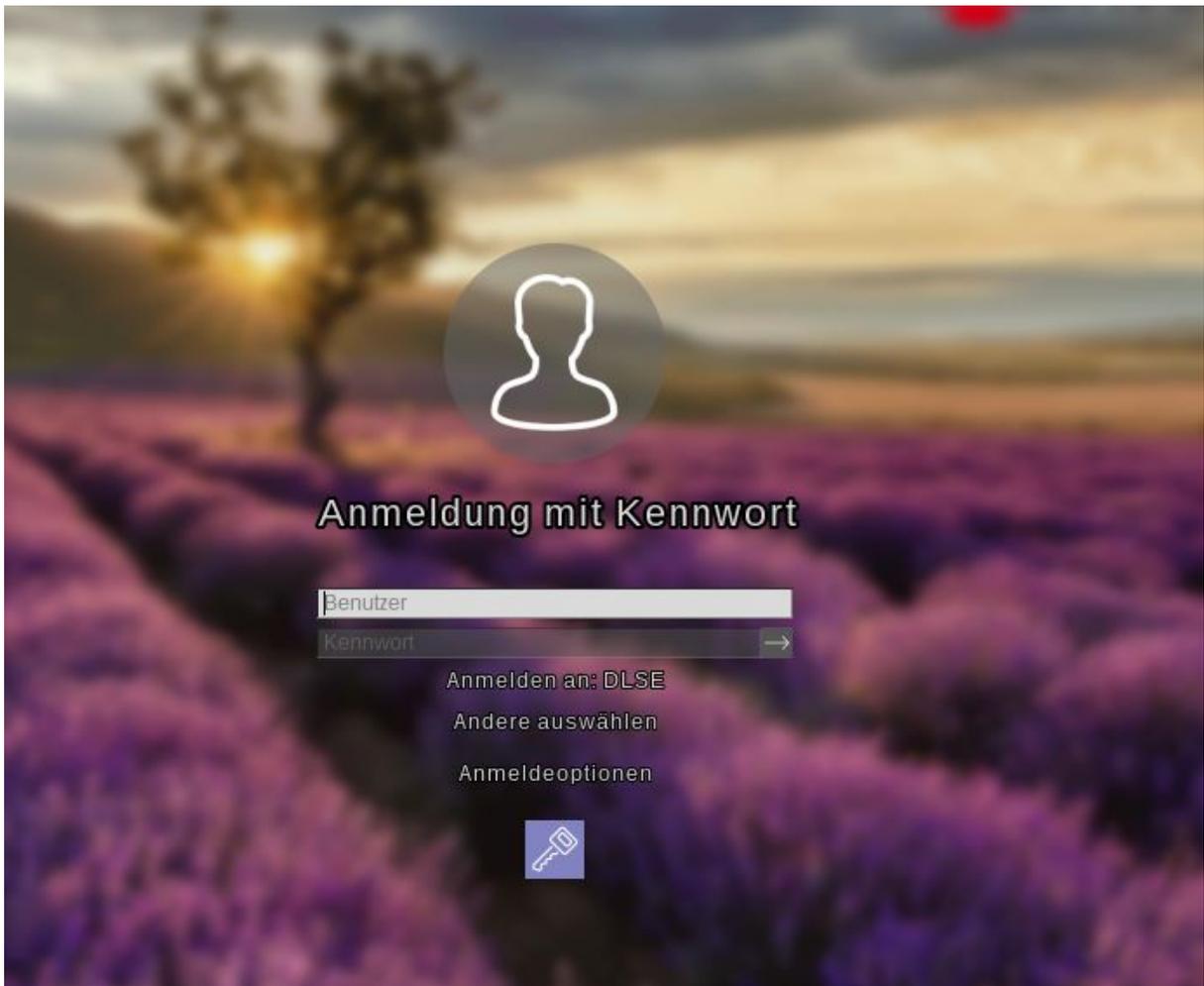


4. Gleichzeitig wird die Verschlüsselung gestartet, ein Neustart oder ein Herunterfahren des Rechners ist von nun an jederzeit möglich.

2.4.2 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.

2.4.3 Netzwerk-Preboot-Authentifizierung

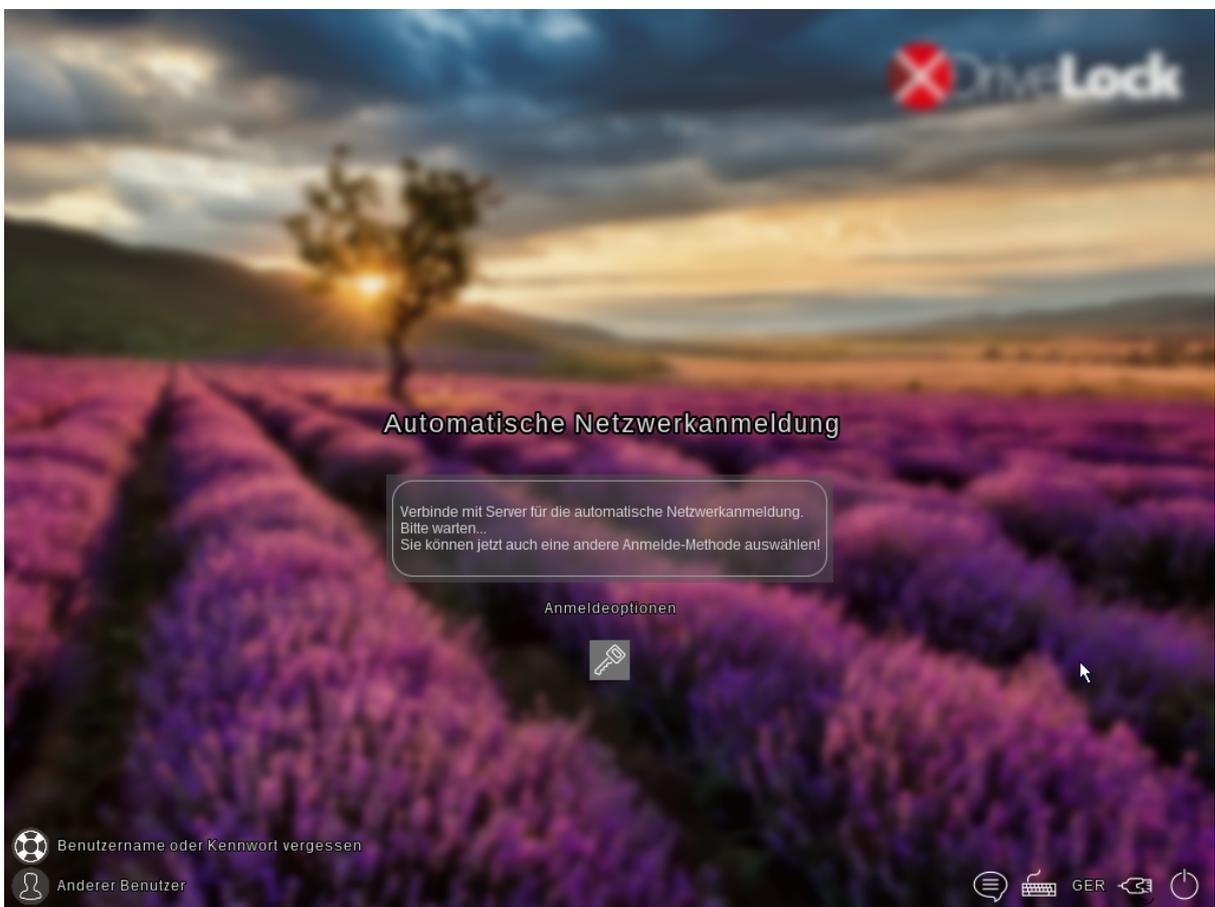
Wenn die Richtlinie mit den [Netzwerk-PBA-Einstellungen](#) auf dem Client-Computer zugewiesen ist und dieser anschließend gestartet wird, kommen folgende Szenarien in Betracht:

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.

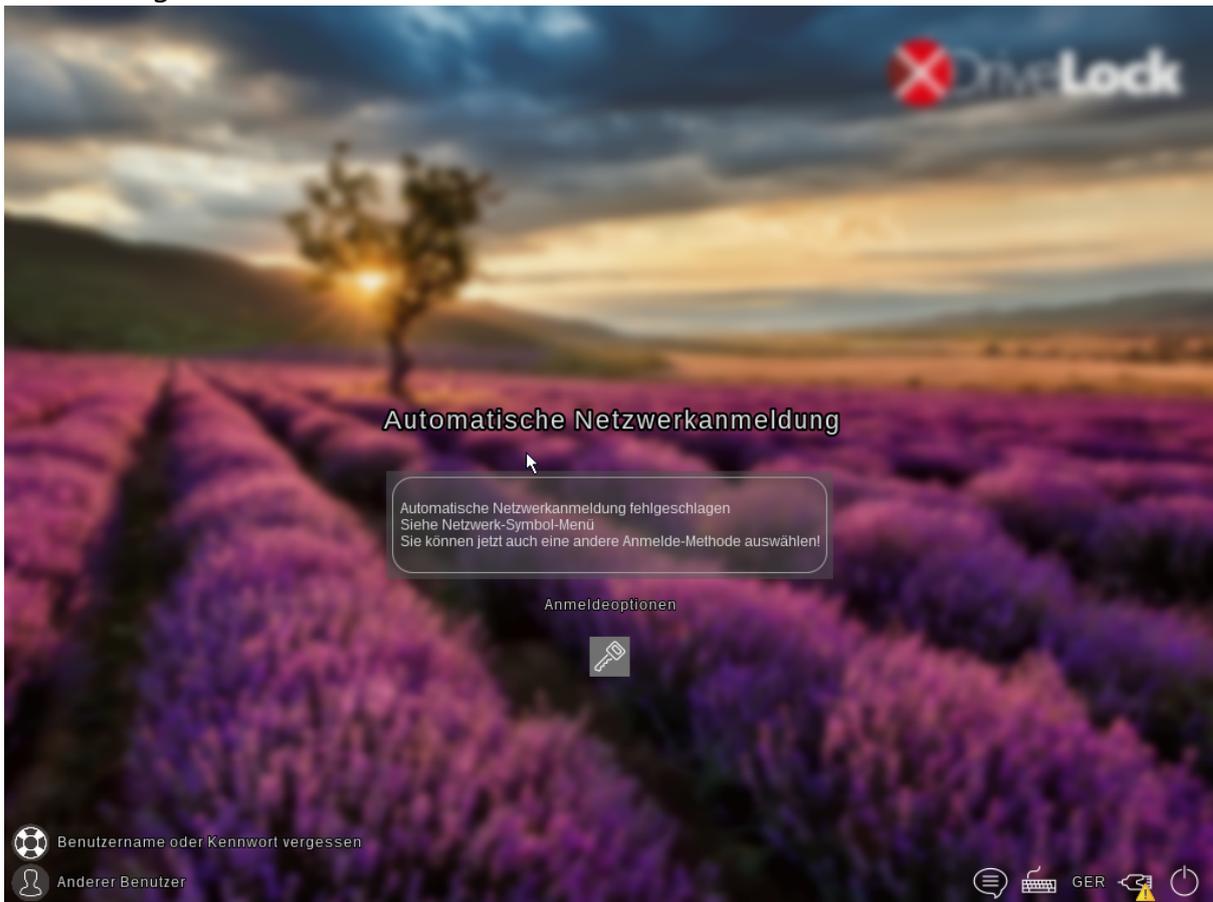


 Hinweis: Durch Anklicken des Schlüssel-Symbols innerhalb von 10 Sekunden kann, sofern erlaubt, zur Anmeldung an der PBA mit Eingabe von Benutzername- und Kennworteingabe umgeschaltet werden.

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

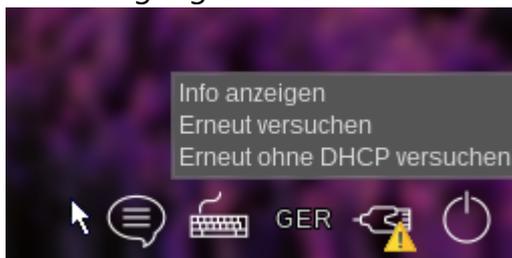
2. Der Client-Computer kann sich nicht mit dem Unternehmensnetzwerk verbinden

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](#).

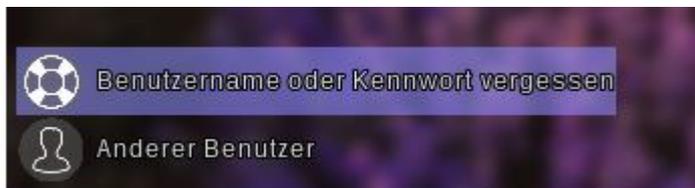
2.4.4 Notfall-Anmeldung mit Wiederherstellungscodes

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.

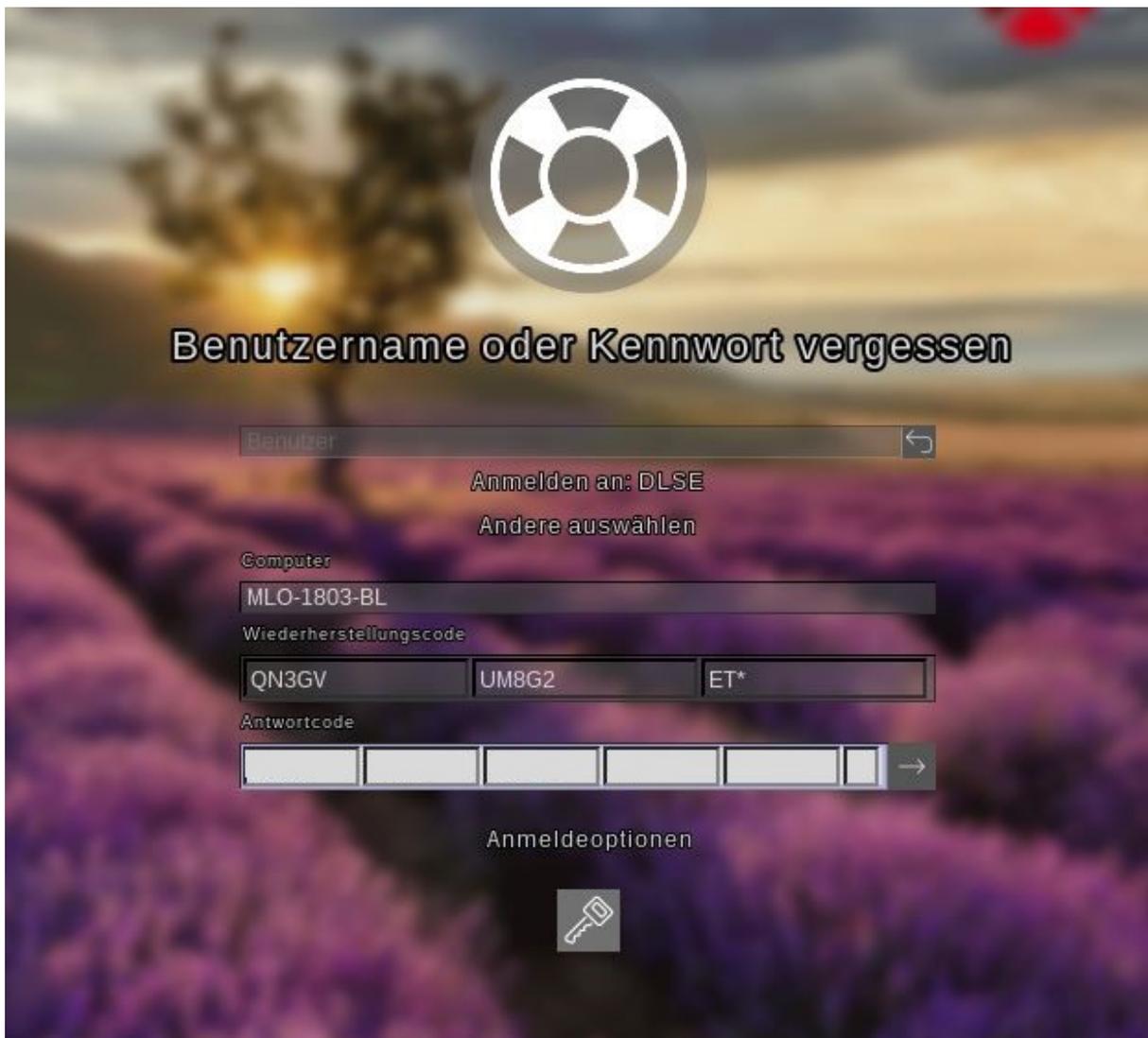
Benutzer und Administrator führen nun folgende Aktionen durch:

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. Wiederherstellungscodes 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.

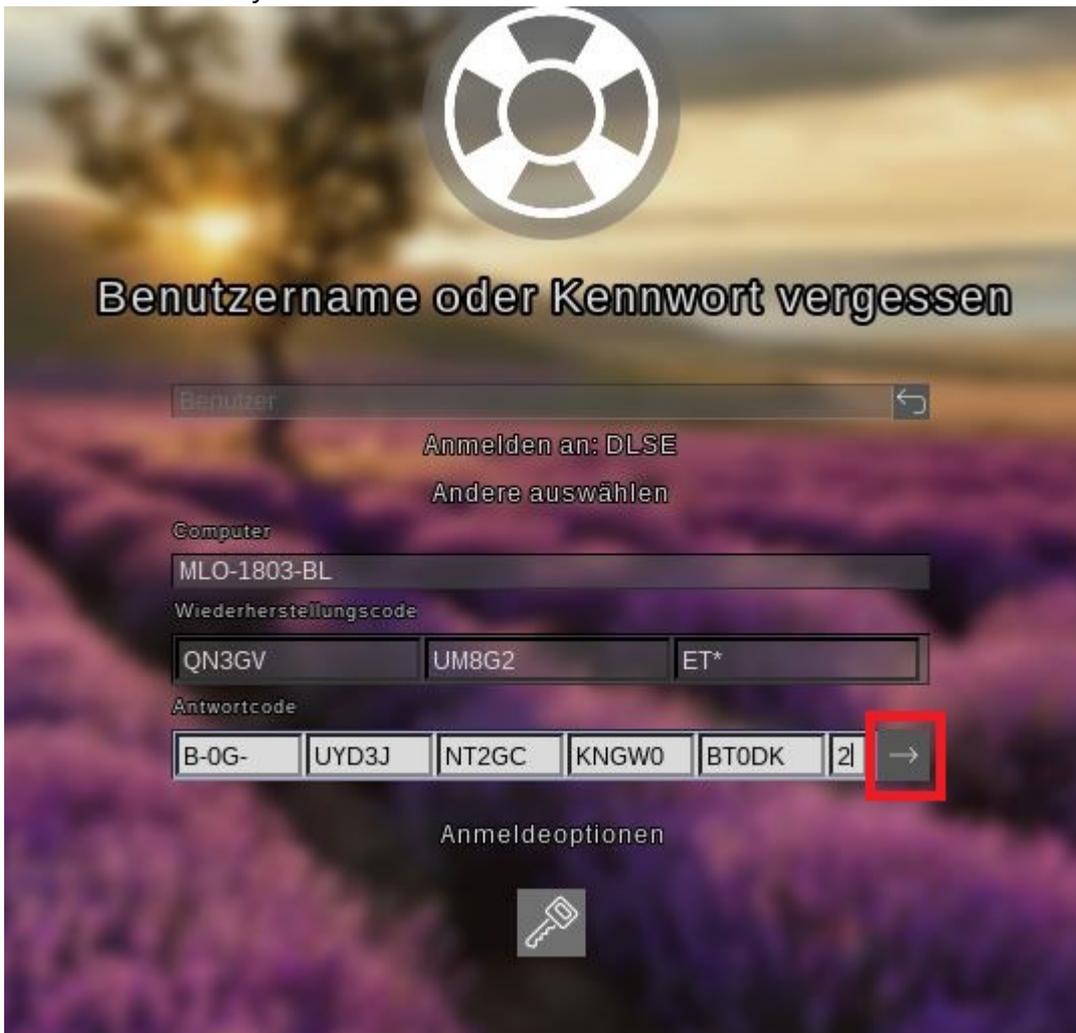
2. Administratoraktion:

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!

2.5 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-logout 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>
    
```

2.6 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

3 DriveLock BitLocker To Go

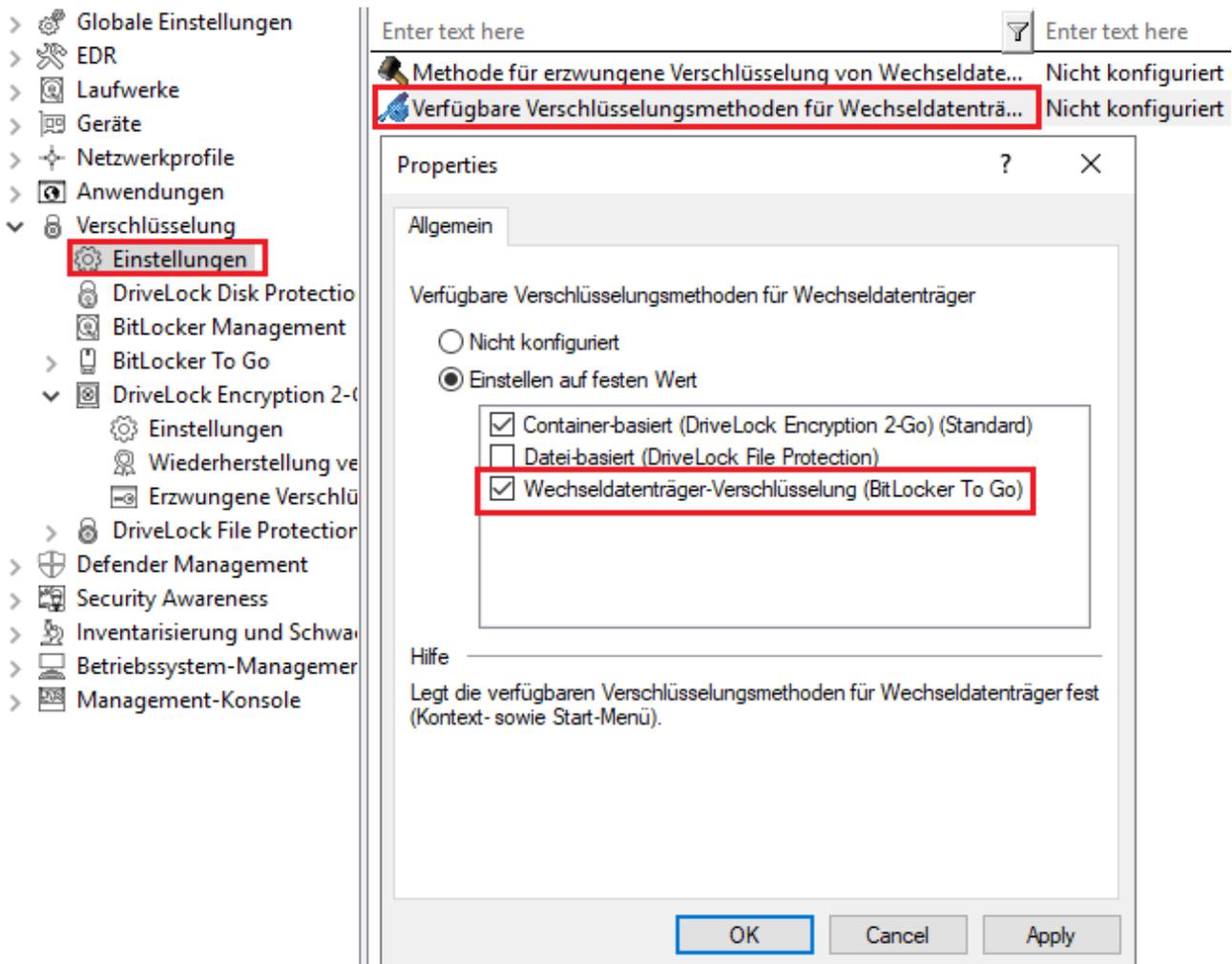
DriveLock BitLocker To Go bietet Ihnen folgende Funktionalitäten:

- 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

3.1 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. Zur Lizenzierung gehen Sie vor, wie im Kapitel [BitLocker Management lizenzieren](#) beschrieben.
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.



3.2 Richtlinienkonfiguration von BitLocker To Go

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**

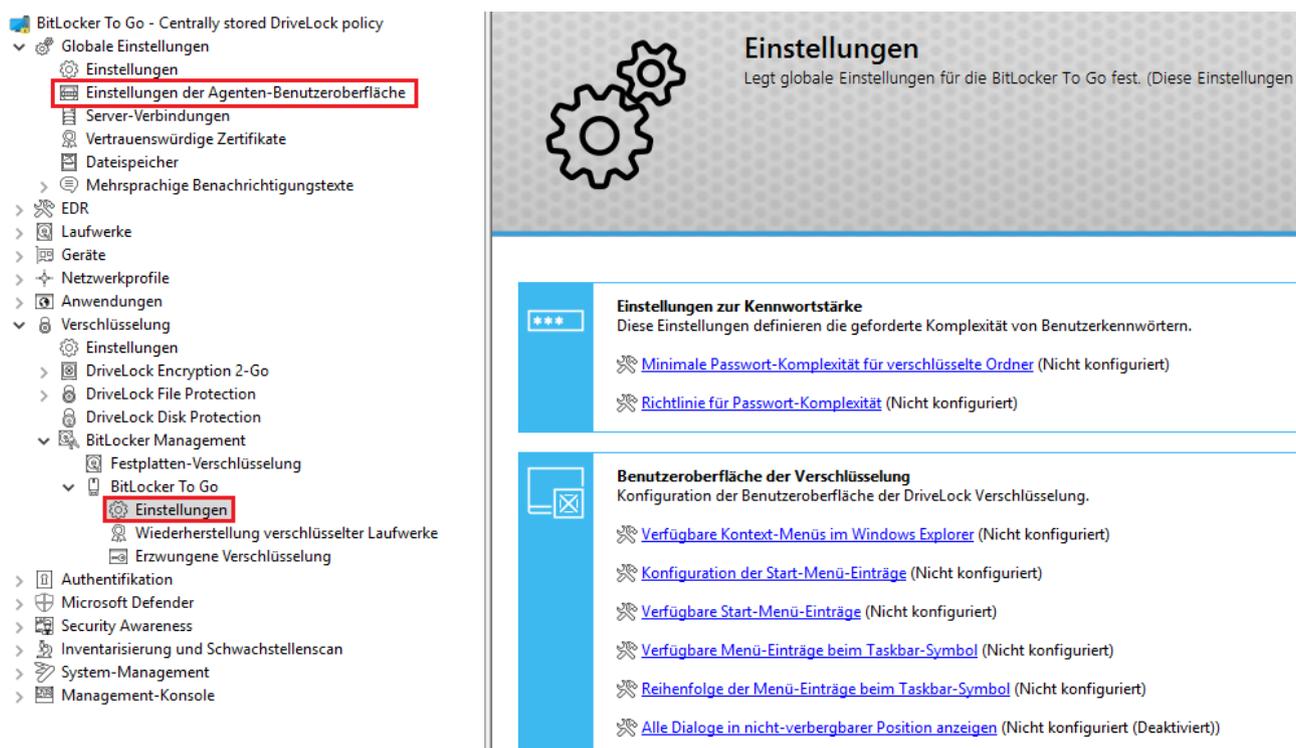
BitLocker To Go angelegt, mit Untermenüs zur Wiederherstellung, Verschlüsselung, Verbindung und Kennwortänderung der jeweiligen USB-Speichermedien.

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\$)

3.2.1 Allgemeine Einstellungen für BitLocker To Go

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



BitLocker To Go - Centrally stored DriveLock policy

- ▼ Globale Einstellungen
 - ⚙️ Einstellungen
 - ⚙️ Einstellungen der Agenten-Benutzeroberfläche**
 - 🌐 Server-Verbindungen
 - 🛡️ Vertrauenswürdige Zertifikate
 - 📁 Dateispeicher
 - 🗨️ Mehrsprachige Benachrichtigungstexte
- > EDR
- > Laufwerke
- > Geräte
- > Netzwerkprofile
- > Anwendungen
- ▼ Verschlüsselung
 - ⚙️ Einstellungen
 - 🔒 DriveLock Encryption 2-Go
 - 🔒 DriveLock File Protection
 - 🔒 DriveLock Disk Protection
 - ▼ BitLocker Management
 - 🔒 Festplatten-Verschlüsselung
 - ▼ BitLocker To Go
 - ⚙️ Einstellungen**
 - 🔄 Wiederherstellung verschlüsselter Laufwerke
 - 📁 Erzwingene Verschlüsselung
- > Authentifikation
- > Microsoft Defender
- > Security Awareness
- > Inventarisierung und Schwachstellenscan
- > System-Management
- > Management-Konsole

Einstellungen
Legt globale Einstellungen für die BitLocker To Go fest. (Diese Einstellungen sind nicht konfigurierbar.)

***** Einstellungen zur Kennwortstärke**
Diese Einstellungen definieren die geforderte Komplexität von Benutzerkennwörtern.

- 🔗 [Minimale Passwort-Komplexität für verschlüsselte Ordner](#) (Nicht konfiguriert)
- 🔗 [Richtlinie für Passwort-Komplexität](#) (Nicht konfiguriert)

Benutzeroberfläche der Verschlüsselung
Konfiguration der Benutzeroberfläche der DriveLock Verschlüsselung.

- 🔗 [Verfügbare Kontext-Menüs im Windows Explorer](#) (Nicht konfiguriert)
- 🔗 [Konfiguration der Start-Menü-Einträge](#) (Nicht konfiguriert)
- 🔗 [Verfügbare Start-Menü-Einträge](#) (Nicht konfiguriert)
- 🔗 [Verfügbare Menü-Einträge beim Taskbar-Symbol](#) (Nicht konfiguriert)
- 🔗 [Reihenfolge der Menü-Einträge beim Taskbar-Symbol](#) (Nicht konfiguriert)
- 🔗 [Alle Dialoge in nicht-verbergbarer Position anzeigen](#) (Nicht konfiguriert (Deaktiviert))

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** im Unterknoten **BitLocker Management**:

- **Minimale Passwort-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 Passwort-Komplexität:**
Definieren Sie hier die minimalen Anforderungen, die Benutzer bei Eingabe eines BitLocker To Go-Kennworts beachten müssen.
- Einstellungen unter **Benutzeroberfläche der Verschlüsselung:**
Alle Einstellungen wirken sich auf die Anzeige von BitLocker To Go im Startmenü, in der Taskleiste oder im Windows Explorer aus.
Weitere Informationen unter [BitLocker To Go auf dem DriveLock Agenten](#).

3.2.2 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.

3.2.2.1 Administrator-Kennwort

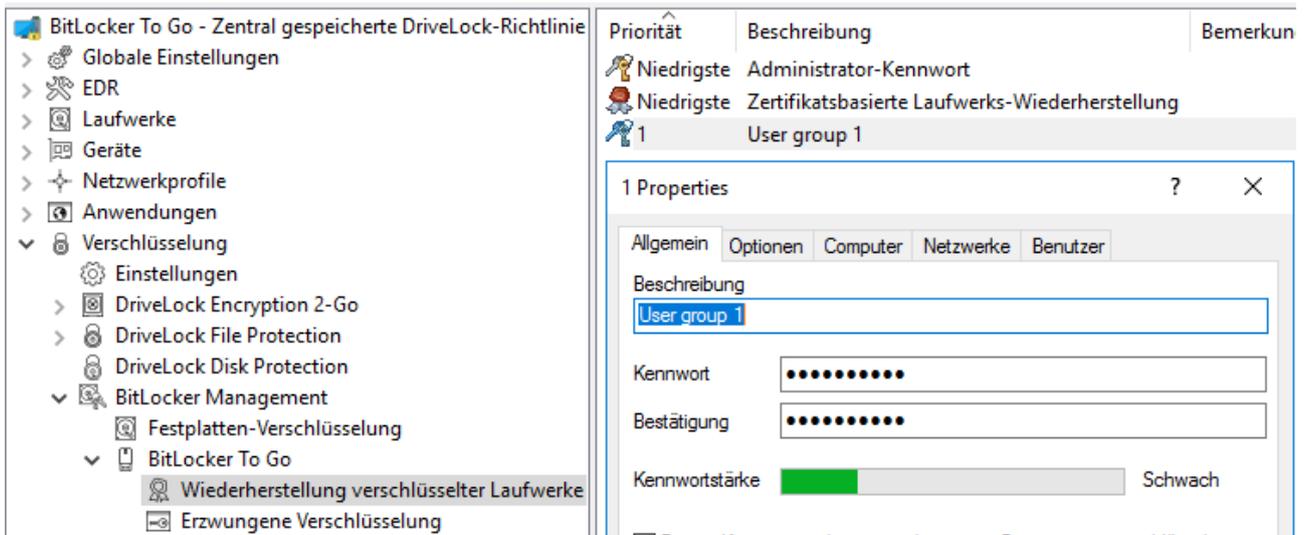
Mithilfe eines zentralen Administrator-Kennworts kann auf verschlüsselte Wechseldatenträger zugegriffen werden.

 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 **Benutzer** oder Benutzergruppen, **Computer** oder **Netzwerke** einschränken. Hierzu geben Sie auf den Reitern im Dialog die entsprechenden Informationen ein. Siehe [Anwendungsfälle](#).



3.2.2.2 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 [Verschlüsselungszertifikate](#).

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 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.

3.2.3 Erzwungene Verschlüsselung

Als erstes legen Sie eine Standard-Verschlüsselungs-Regel an. Sie können dann bei Bedarf weitere Regeln für bestimmte Benutzer, Gruppen, Computer oder Netzwerke anlegen. Siehe [Anwendungsfälle](#).

Bei Anlage 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 Systemen 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.

3.3 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.

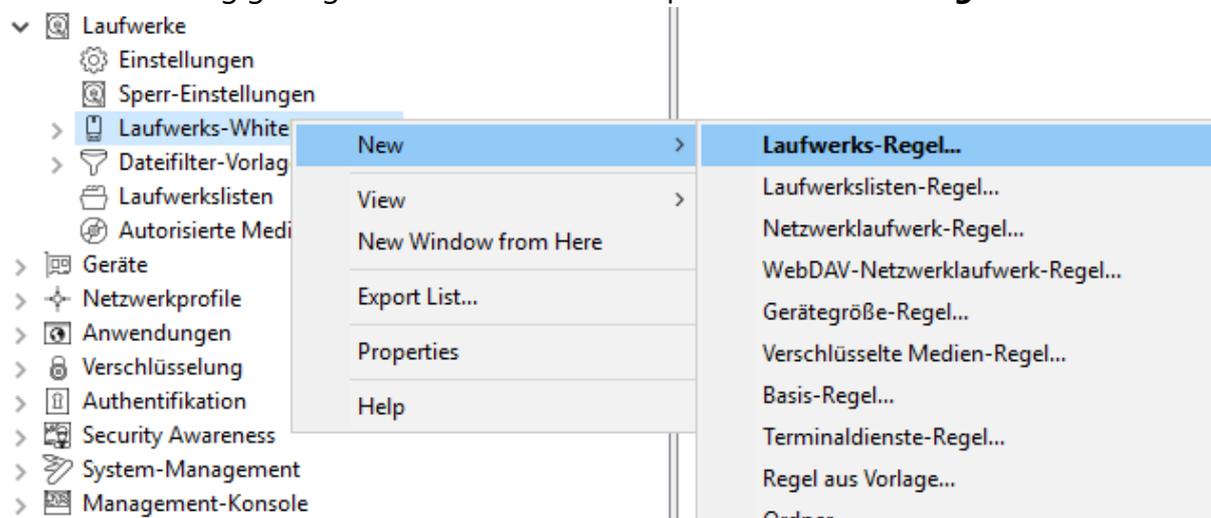
1. Erstellen Sie eine Richtlinie (oder öffnen Sie eine bereits vorhandene), in der Sie die Einstellungen für BitLocker To Go setzen wollen.

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

- 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.

- Wählen Sie die Option **Verfügbare Verschlüsselungsmethoden**.
- 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.
- Öffnen Sie den Knoten **Laufwerke**. Bei den **Sperr-Einstellungen** für **USB-angeschlossene Laufwerke** übernehmen Sie die Standardeinstellung **Nicht konfiguriert (Gesperrt)**.
- Öffnen Sie aus dem Unterknoten **Laufwerks-Whitelist-Regeln** das Kontextmenü, wie in der Abbildung gezeigt. Hier wählen Sie die Option **Laufwerks-Regel** aus.



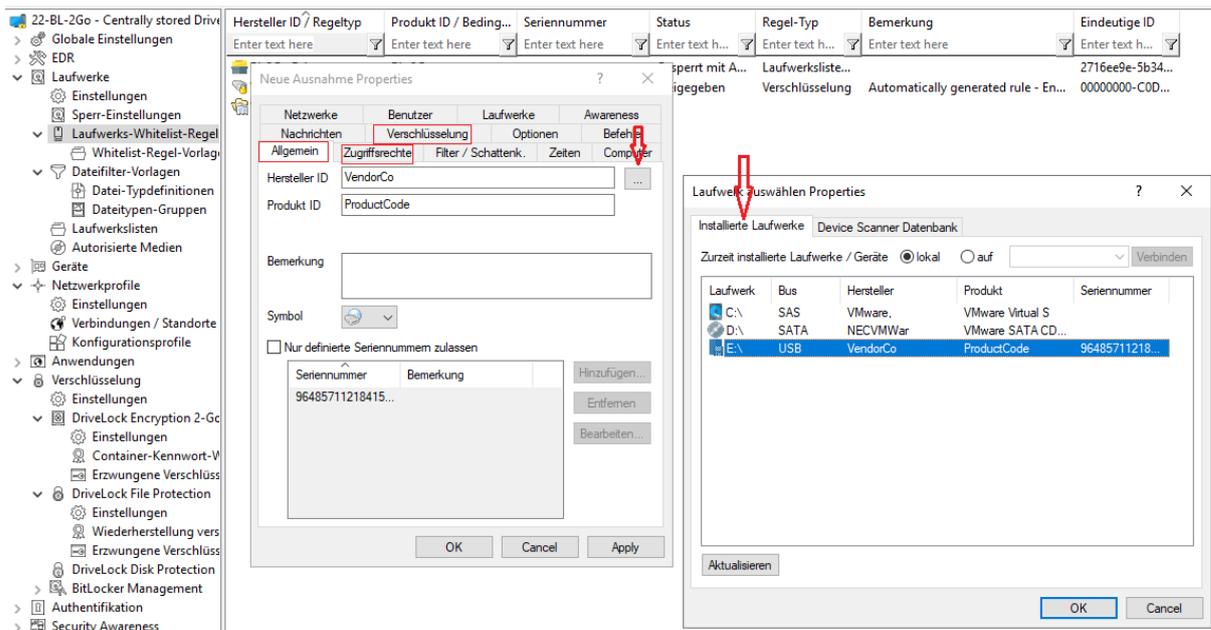
- Erstellen Sie eine Laufwerks-Regel für das entsprechende USB-Laufwerk. Ein Beispiel finden Sie [hier](#).
- Als nächstes öffnen Sie wieder den Knoten **Verschlüsselung** und darin den Unterknoten **BitLocker Management**. Hier gehen Sie direkt zu **BitLocker To Go** und wählen zunächst die Option **Wiederherstellung 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.

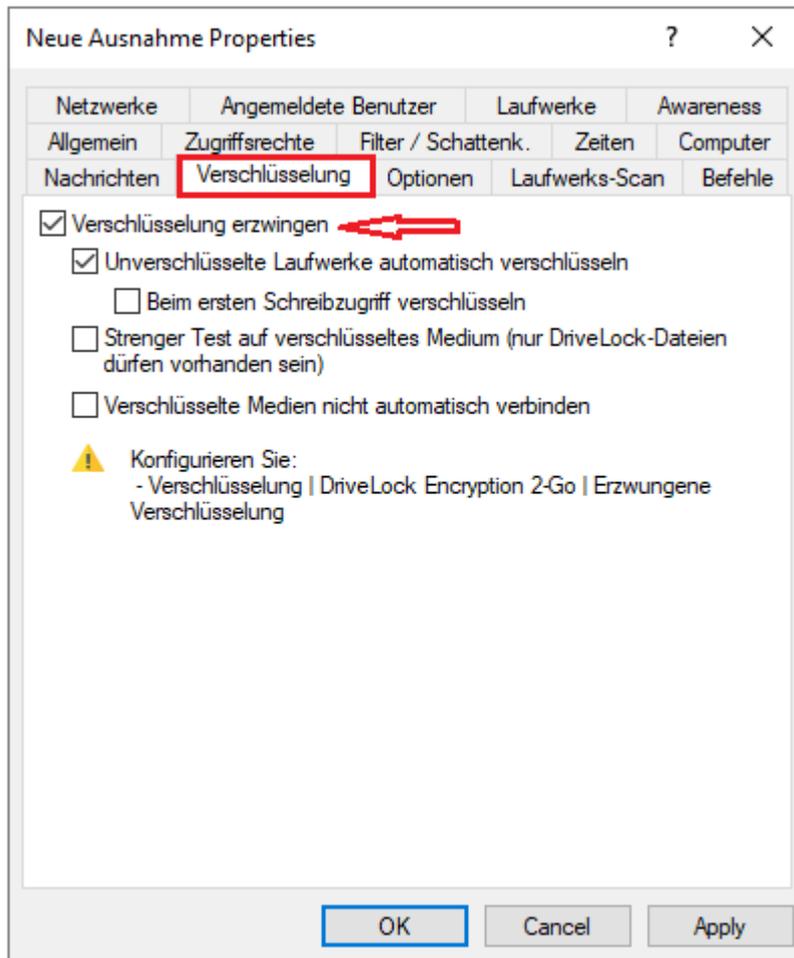
3.3.1 Laufwerks-Whitelist-Regel anlegen

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.

3.4 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-

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

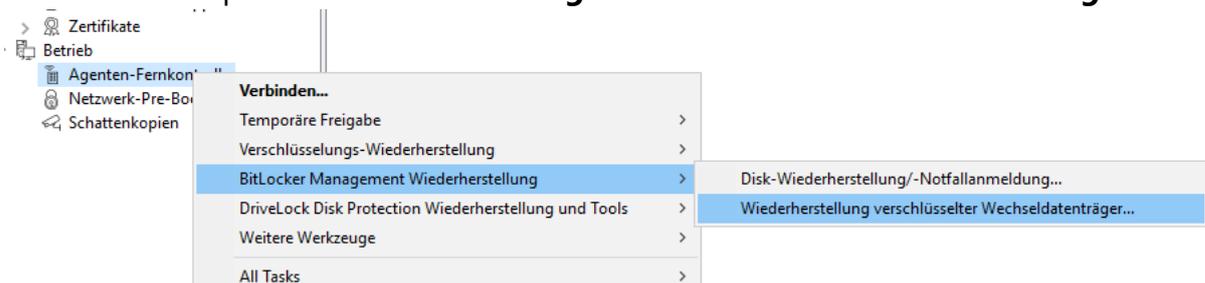
Das Kennwort kann auch dann zurückgesetzt werden, wenn der Client-Computer sich aktuell nicht im Unternehmensnetzwerk befindet.

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.

3.4.1 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.

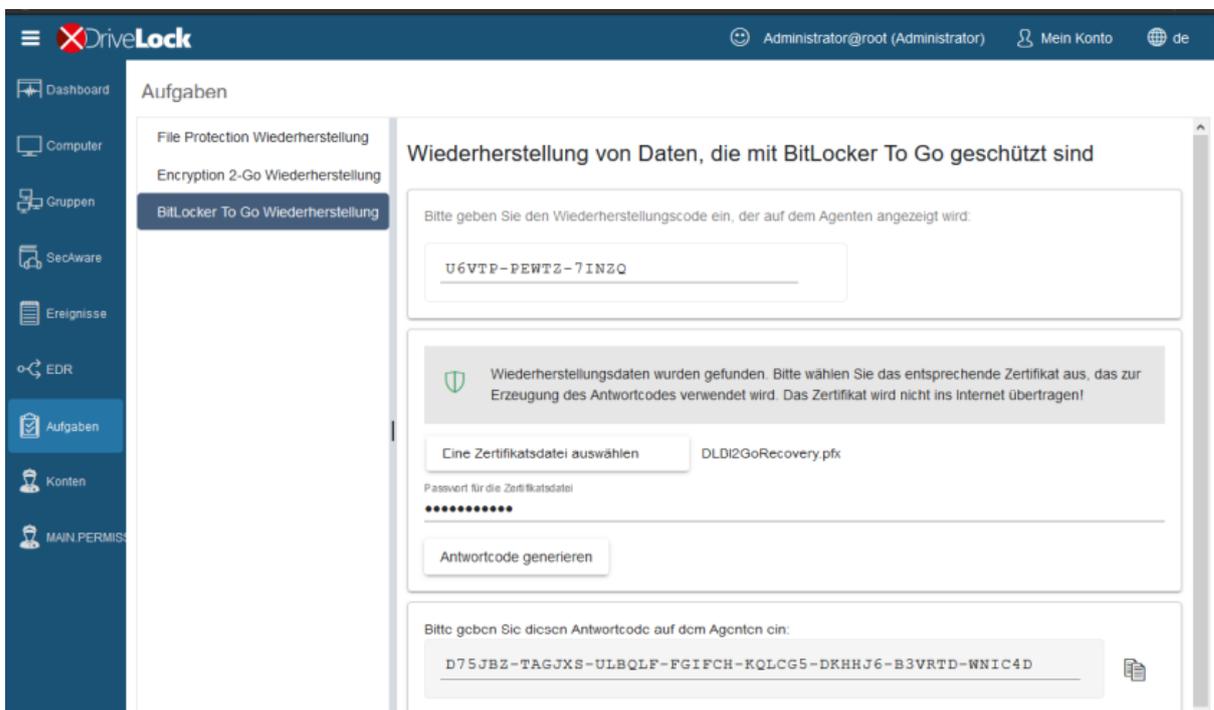
- Der Benutzer gibt nun seinerseits den **Antwortcode** am Client-Computer ein. Im anschließenden Dialog kann ein neues Benutzerkennwort für das USB-Speichermedium vergeben werden.

3.4.2 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:

- Öffnen Sie das **DOC** (aus dem DriveLock Control Center oder über Ihren Browser).
- Wählen Sie den Bereich **Aufgaben** aus und hier das Untermenü **BitLocker To Go Wiederherstellung**.
- Der Benutzer am Client-Computer hat in der Zwischenzeit den Wiederherstellungsassistenten aufgerufen und sich den **Anforderungs- bzw. Wiederherstellungscodes** anzeigen lassen. Lassen Sie sich diesen übermitteln.
- Geben Sie dann den **Anforderungs- bzw. Wiederherstellungscodes** in Ihre DOC-Maske ein.



- Wählen Sie die passende **Zertifikatsdatei** aus und geben das dazugehörige Kennwort ein.
- Klicken Sie auf **Antwortcode generieren** und teilen Sie diesen dem Benutzer mit.

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

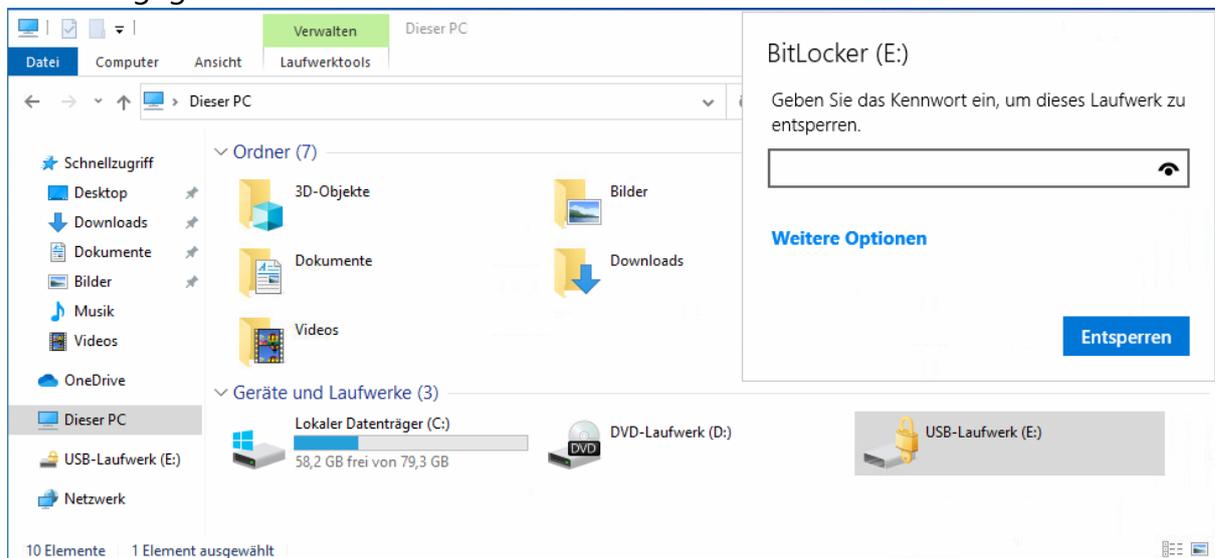
3.5 DriveLock Agent

3.5.1 BitLocker To Go auf dem DriveLock Agenten

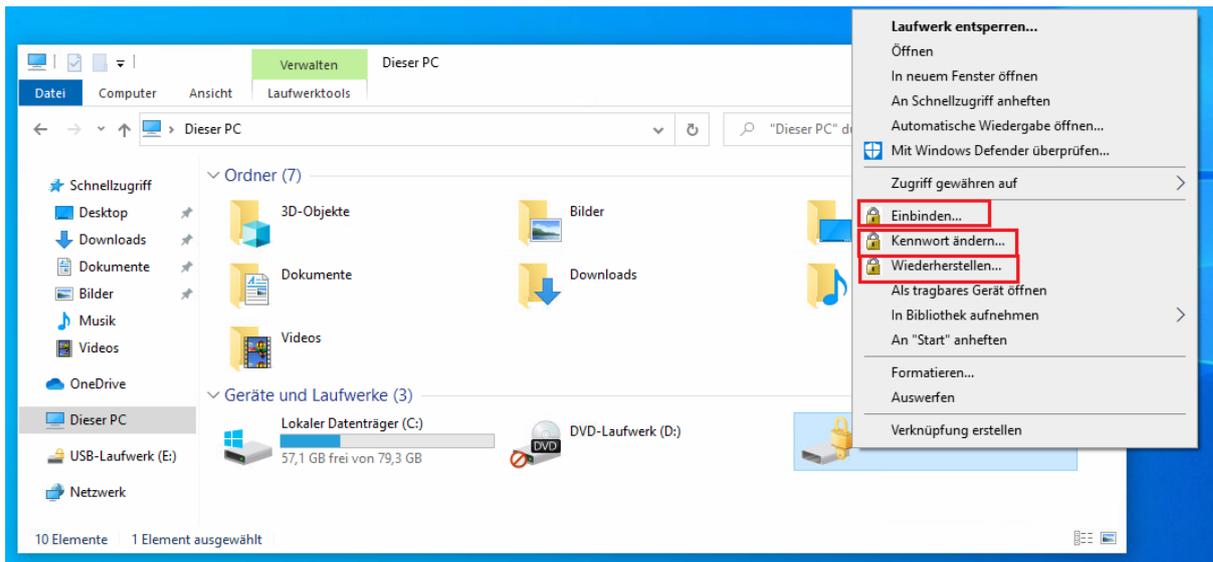
Beim Einstecken eines externen USB-Speichermediums oder externen Laufwerks am DriveLock Agenten können dem Benutzer je nach Richtlinien-Einstellung folgende Optionen angeboten werden:

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.

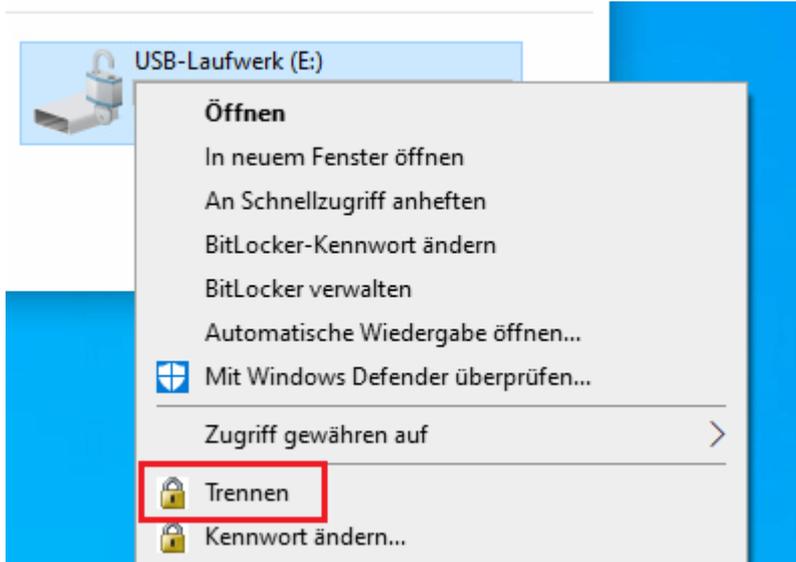
- **Wiederherstellen...**

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

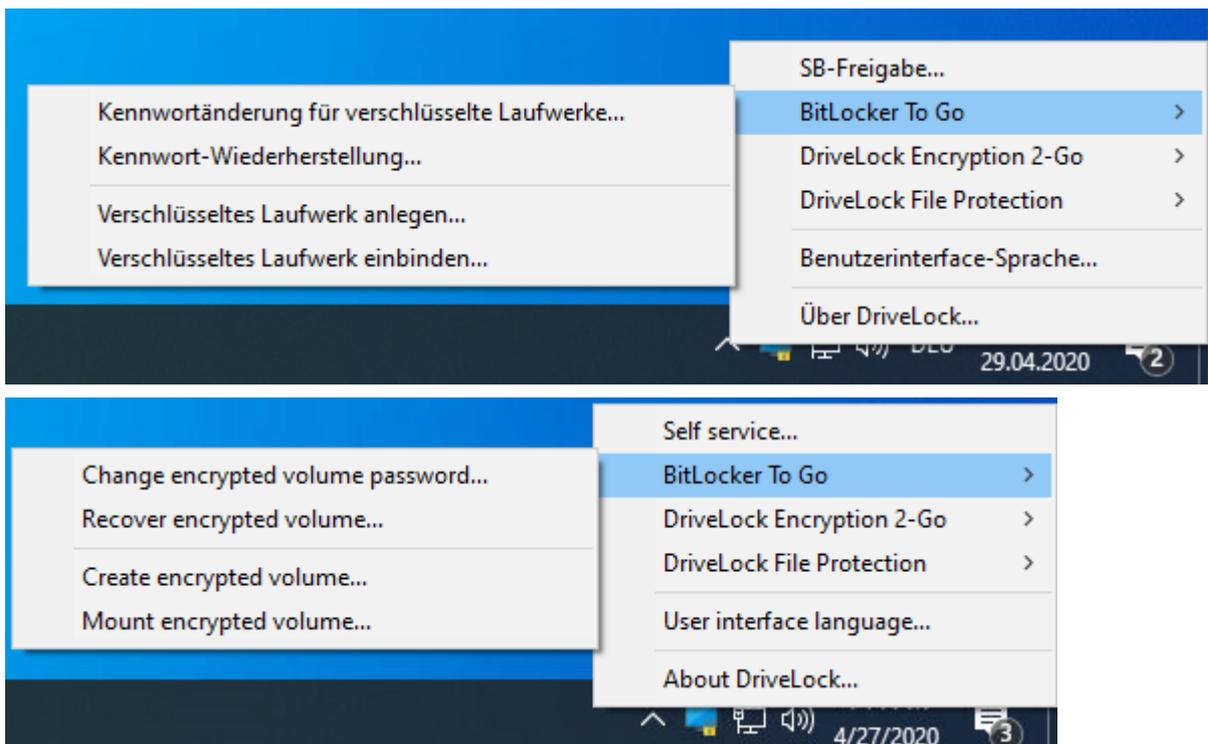
- **Trennen**

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:



3.6 Verschiedene Anwendungsfälle

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

- Vergabe des Administrator-Kennworts
- Erzwungene Verschlüsselung

3.6.1 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 **Benutzer, Computer** und **Netzwerk** gesetzten Filtermöglichkeiten.

3.6.2 Verschlüsselungs-Regeln

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

Index

A

Authentifizierungstyp 27, 38

B

BitLocker Lizenz 10

C

Copyright 111

D

Datenpartition 28

E

Entschlüsselung 17, 21, 35

F

Festplatten 6, 17, 27, 34, 38-39, 47

H

Hardware-Verschlüsselung 18

I

Index 109

K

Kennwortoptionen 30, 38

P

Pre-Boot-Authentifizierung 27, 38, 48, 51

privater Schlüssel 14, 23

S

Systempartition 28, 39, 43, 51

V

Verschlüsselung 6, 12, 17, 30, 38, 41, 48-49

Verschlüsselungsalgorithmus 18, 39

Verschlüsselungsmethoden 18

Verschlüsselungszertifikate 12-13, 38

W

Wiederherstellung 12-13, 22, 39, 41

Wiederherstellungsschlüssel 42

Z

Zertifikatsspeicher 12, 42

Zuweisung 48

Copyright

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

© 2021 DriveLock SE. Alle Rechte vorbehalten.