Aagon

E-BOOK

BITLOCKER MIT GRUPPENRICHTLINIEN, POWERSHELL UND MANAGE-BDE VERWALTEN

Dezember 2023

www.aagon.com

Inhalt

Über den Autor

Windows Pro
Windows, Virtualisierung und Cloud für Profis

Das E-Book wurde erstellt von Wolfgang Sommergut – Fachautor, Berater und Konferenzsprecher zu verschiedenen Themen der IT.

Einleitung

BitLocker ist eine unverzichtbare Komponente in jedem Sicherheitskonzept für Firmen-Notebooks. Das Feature verhindert, dass vertrauliche Daten nach dem Verlust oder Diebstahl der Hardware in die falschen Hände geraten.

Die Verschlüsselung von Laufwerken ist aber auch bei Desktop-PCs und sogar auf Windows Server ratsam, wenn die Geräte nicht verlässlich vor dem physischen Zugriff von potenziellen Angreifern geschützt sind.

Wohlbekannte Tricks, um das Passwort des lokalen Administrators zurückzusetzen und sich damit am Rechner anzumelden, funktionieren dann nicht mehr.

Mobile Datenträger stellen ein besonderes Risiko für den unerwünschten Abfluss von Daten dar. Auch dem kann BitLocker einen Riegel vorschieben, indem alle im Unternehmen verwendeten USB-Laufwerke zwingend verschlüsselt werden.

BitLocker-Management mit den Bordmittel

In einem professionellen Umfeld überlässt man es normalerweise nicht den Endbenutzern, eine derartig kritische Sicherheitsfunktion in Eigenregie zu verwalten. Dies würde nicht nur den gewünschten Schutz beeinträchtigen, sondern auch zu häufigen Helpdesk-Anrufen führen, etwa wenn sich Benutzer ausgesperrt haben und den Recovery Key nicht mehr finden.

Microsoft liefert daher mit dem Betriebs¬system auch die Mittel für die zentrale Verwaltung von BitLocker aus. Dabei handelt es sich neben den üblichen Verdächtigen wie Gruppenrichtlinien und PowerShell um das Dienstprogramm manage-bde.

Sie bieten eine Reihe von Optionen, die etwa das Benutzererlebnis, den Algorithmus oder den zu verschlüsselnden Bereich auf dem Datenträger betreffen. Im Zentrum steht jedoch die Verwaltung der Mechanismen, die den Key für die Laufwerks¬verschlüsselung schützen.

Management der Key Protectors im Vordergrund

BitLocker verwendet nämlich ein symmetrisches Verfahren, bei dem die Daten mit dem gleichen Key ver- und entschlüsselt werden. Entsprechend steht und fällt der Schutz durch BitLocker mit dem Zugang zum verwendeten Schlüssel. Dieser wird in letzter Instanz durch die so genannten Key Protectors geregelt, die ihrerseits den Volume Master Key (VMK) codieren.

Bei ihnen geht es nicht nur um maximale Sicherheit, sondern sie müssen auch in der Lage sein, BitLocker an unterschiedliche Nutzungsszenarien anzupassen. So kann es in sicheren Umgebungen sinnvoll sein, Laufwerke automatisch zu entsperren, während in Branchen mit hohen Anforderungen eine Authentifizierung über mehrere Faktoren angebracht erscheint.

Die Key Protectors stellen somit ein zentrales Konzept von BitLocker dar und Admins sind damit spätestens dann konfrontiert, wenn Benutzer ihre Rechner nicht entsperren können. Allerdings sollten diese Schutzmechanismen nicht erst die Aufmerksamkeit der Systemverwaltung bekommen, wenn Probleme auftreten.

Vielmehr gehört es zu einer guten Planung des BitLocker-Einsatzes, sich vorab Gedanken darüber zu machen, wie man den VMK schützen möchte. Auf Betriebssystemlaufwerken fällt diese Entscheidung meistens zugunsten von TPM plus PIN aus.

Für Datenlaufwerke und Wechseldatenträger gibt es eine Reihe von Optionen, bei deren Wahl die Anforderungen der jeweiligen Umgebung entscheidend sind.

Bordmittel mit Defiziten

Wie bei anderen Systemkomponenten auch, lassen sich grundsätzlich zwar alle Funktionen von BitLocker mit den Bordmitteln verwalten. Aber die Kombination aus Gruppenrichtlinien, PowerShell und manage-bde bietet beispielsweise keine Berichte geschweige denn Dashboards, die auf einen Blick zeigen, ob auf einzelnen Rechnern Probleme aufgetreten sind und diese somit ungeschützt sind.

Außerdem kann man mit den Gruppenrichtlinien das Feature zwar konfigurieren, aber die Verschlüsselung nicht starten. Daher greifen Admins für diesen Zweck in der Regel zu Scripts. Ausgewachsene Lösungen für das Client-Management bieten hier klare Vorteile.

BitLocker Key Protectors verwalten

BitLocker nutzt symmetrische Verfahren zur Verschlüsselung von Laufwerken. Der dafür eingesetzte Key ist durch zwei Verschlüsselungsebenen geschützt. Auf der obersten Schicht gewähren Protectors über verschiedene Mechanismen den Zugang zu den Datenträgern. Nicht alle sind jedoch gleich sicher oder eignen sich für sämtliche Laufwerke.

Microsoft bezeichnet den Schlüssel, mit dem BitLocker die Sektoren der Laufwerke verschlüsselt, als Full Volume Encryption Key (FVEK). Wer in dessen Besitz gelangt, kann die damit codierten Daten entschlüsseln. Entsprechend wichtig ist es, den FVEK vor unbefugtem Zugriff zu schützen.

BitLocker verschlüsselt den FVEK seinerseits mit dem Volume Master Key (VMK) und legt beide auf dem verschlüsselten Laufwerk ab, und zwar in einem Bereich des Volume-Headers, der unverschlüsselt bleibt. Andernfalls würde sich BitLocker selbst aussperren.

Protectors schützen den Volume Master Key

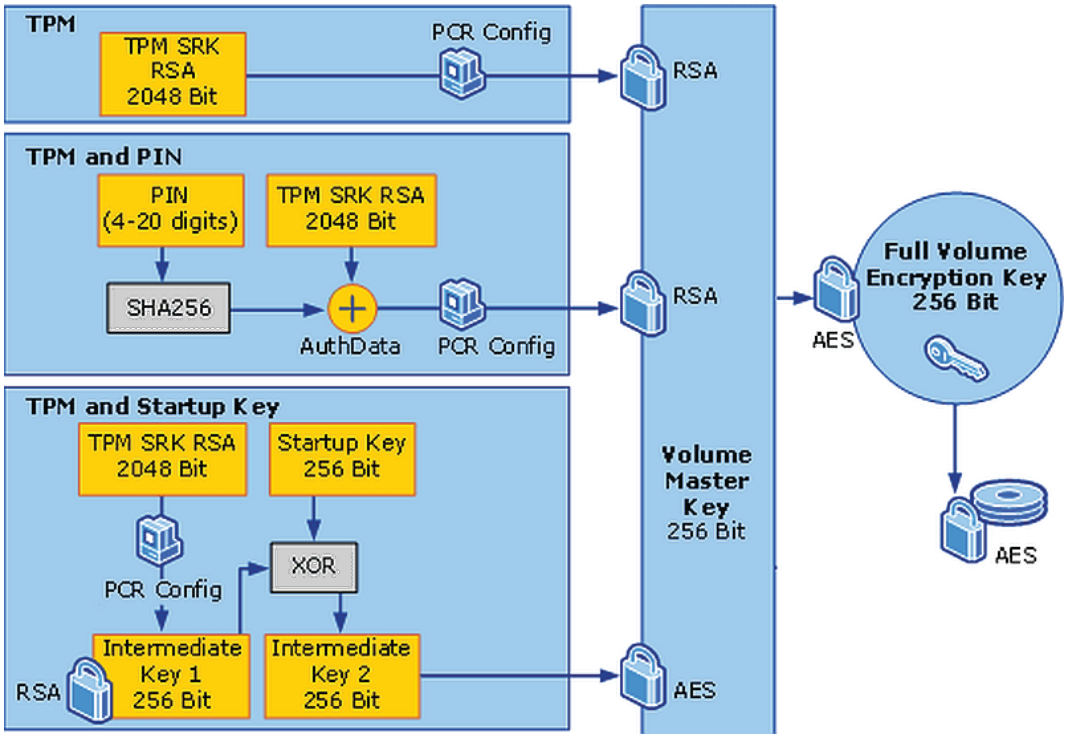
Um an den FVEK zu gelangen, benötigt man also den VMK. Dieser sollte daher ebenfalls vor unautorisiertem Zugriff geschützt sein. Für diese Aufgabe verwendet BitLocker die folgenden Protectors:

- TPM
- TPM mit PIN
- TPM mit Start-Key
- TPM mit PIN und Start-Key
- Passwort
- Wiederherstellungspasswort
- Externer Recovery Key
- Zertifikat für Wiederherstellungsagenten
- Network Unlock
- Benutzer oder Gruppe aus dem Active Directory (SID)

Jeder Protector erhält eine eigene Kopie des VMK, den er mit seinen eigenen Mitteln verschlüsselt.

TPM, PIN und Startschlüssel

Die Kombination aus TPM, PIN oder Startschlüssel ist ausschließlich für das Betriebssystemlaufwerk vorgesehen. Standardmäßig nutzt BitLocker nur das TPM, so dass der Rechner ohne Benutzereingriff entsperrt wird.



Key Protectors auf Basis des Trusted Platform Modules

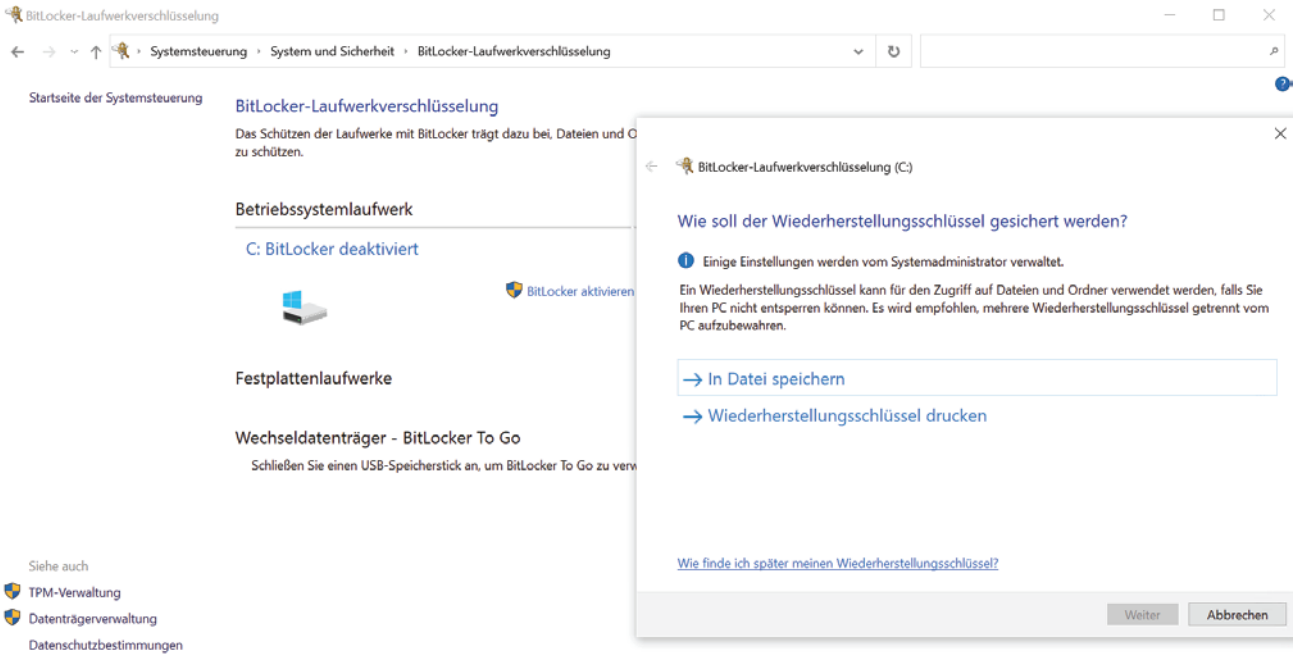
Das TPM verschlüsselt den MVK mit seinem Public Key und entschlüsselt ihn beim Hochfahren des Rechners mit seinem Private Key. Zusätzlich untersucht es die Integrität des Systems mit Hilfe der in den Platform Configuration Register (PCR) gespeicherten Parameter. Nur wenn der Rechner diese Prüfung besteht, gibt das TPM den VMK frei.

Ergänzt man die TPM-Authentifizierung um eine PIN oder einen Startschlüssel, dann muss der VMK auch von diesen Mechanismen erfolgreich entschlüsselt werden, bevor er zugänglich ist.

Wiederherstellungsschlüssel

Schlägt das Entsperren über den konfigurierten Protector fehl, etwa weil sich die Hardware verändert oder der Benutzer die PIN vergessen hat, dann benötigt man eine alternative Option, um an den VMK zu gelangen.

Aus diesem Grund generiert BitLocker bei seiner Aktivierung per Voreinstellung ein 48-stelliges numerisches Recovery Password. Dieses könnte man theoretisch auch als einzigen Protector verwenden und bei jedem Booten des Rechners eingeben, aber dies ist nicht praktikabel.

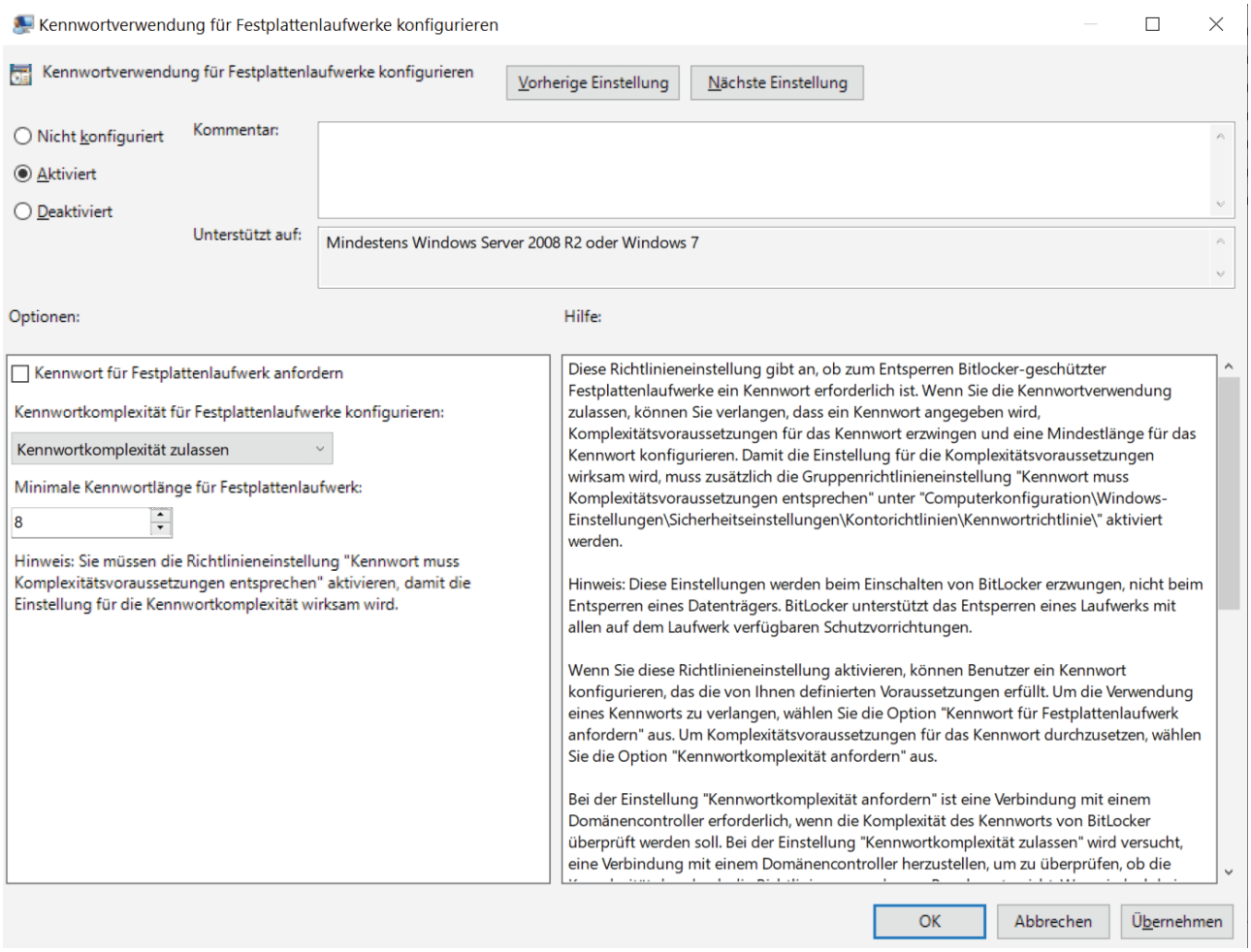


Wenn nicht anders durch Gruppenrichtlinien vorgegeben,
erstellt BitLocker bei seiner Aktivierung ein Recovery Password

Wenn der Wiederherstellungsschlüssel in die Hände eines Angreifers gerät, dann kann er im Recovery Mode alleine damit das Laufwerk entsperren. Daher ist eine sichere Aufbewahrung des Keys ausschließlich für den Notfall essentiell. Ist der Rechner Mitglied in einer Domäne, dann kann man dafür das Active Directory als Speicher nutzen.

Passwörter

Während die Kombination aus TPM und PIN das beste Verhältnis aus Sicherheit und Benutzerkomfort bietet, gilt für ein Passwort das Gegenteil. Es sorgt für den schwächsten Schutz und seine Verwendung ist zudem nicht komfortabel, wenn es die nötige Komplexität hat. Diese kann man per Gruppenrichtlinie vorgeben.

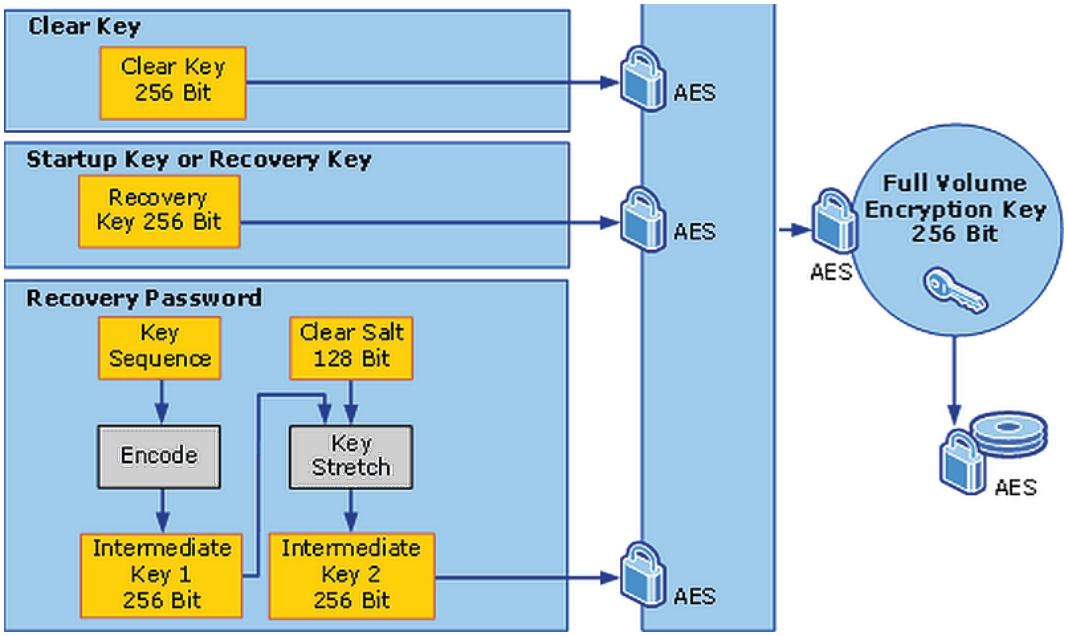


Die Komplexität von Passwörtern lässt sich per Gruppenrichtlinie vorgeben

BitLocker lässt zudem beliebig viele Fehlversuche zu, was die Möglichkeit für Brute-Force-Attacken eröffnet. Aus diesem Grund ist ein Passwort per Voreinstellung als Protector für Systemlaufwerke nicht zulässig, wenn nicht zusätzlich ein TPM konfiguriert wurde.

Externer Key

BitLocker kennt zwei Arten von Schlüsseln, die auf USB-Laufwerken gespeichert werden, nämlich den Startup Key und den Recovery Key. Ersterer lässt sich mit einem TPM kombinieren oder auf alten PCs ohne TPM alleine einsetzen. Der Wiederherstellungsschlüssel dient hingegen für den Notfall.



Optionen zum Entsperren eines verschlüsselten Laufwerks.
Ein Clear Key liegt beim Pausieren von BitLocker vor

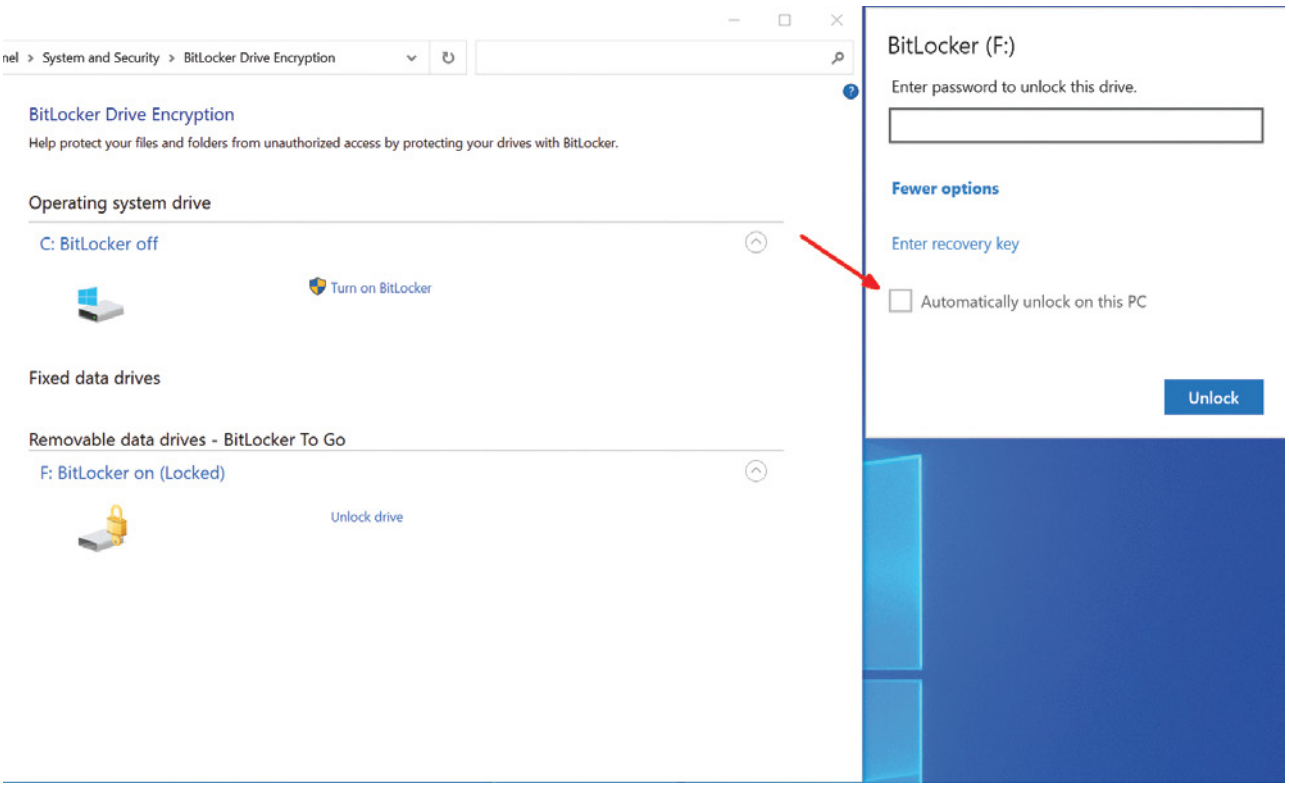
Technisch scheint es keinen großen Unterschied zwischen beiden zu geben, denn der Hilfetext von manage-bde beschreibt *SaveExternalKey*, den gemeinsamen Parameter für beide Typen, folgendermaßen:

Diese externen Schlüsseldateien können als Systemstart- oder Wiederherstellungsschlüssel verwendet werden.

Auto Unlock und SID-Protector

Beide Mechanismen vereinfachen den Zugang zu Datenlaufwerken, weil sie Benutzern die Eingabe eines Passworts ersparen. Sie sind jedoch an bestimmte Bedingungen geknüpft.

Das automatische Entsperren setzt voraus, dass das Systemlaufwerk ebenfalls mit BitLocker geschützt ist. Den Key, mit dem der VMK des Datenlaufwerks verschlüsselt wird, legt Windows nämlich in der Registry ab. Ein ungeschütztes Laufwerk wäre dafür ein schlechter Speicherort.



Auto Unlock für Daten und Wechsellaufwerke über das BitLocker-Management aktivieren

Der Protector *ADAccountOrGroup* (auch SID genannt) entsperrt ein Datenlaufwerk automatisch, wenn die dafür konfigurierten Gruppen oder Benutzer aus dem Active Directory angemeldet sind. Jeder andere User, der sich auf dem Rechner einloggt, erhält keinen automatischen Zugang zum betreffenden Datenträger.

Recovery Agent

Wiederherstellungsagenten eignen sich ebenfalls nur für Daten-, aber nicht für Systemlaufwerke. Letztere lassen sich damit nur dann entsperren, wenn man den Rechner von einem anderen Datenträger bootet und wie ein Datenlaufwerk anspricht.

Das Zertifikat für Wiederherstellungsagenten muss im lokalen Store jedes Rechners gespeichert werden, auf dem man ein Laufwerk entsperren möchte. Daher eignet sich diese Technik beispielsweise sehr gut, wenn der Helpdesk verschlüsselte USB-Sticks von Mitarbeitern entgegennimmt, die das Passwort dafür vergessen haben.

Network Unlock

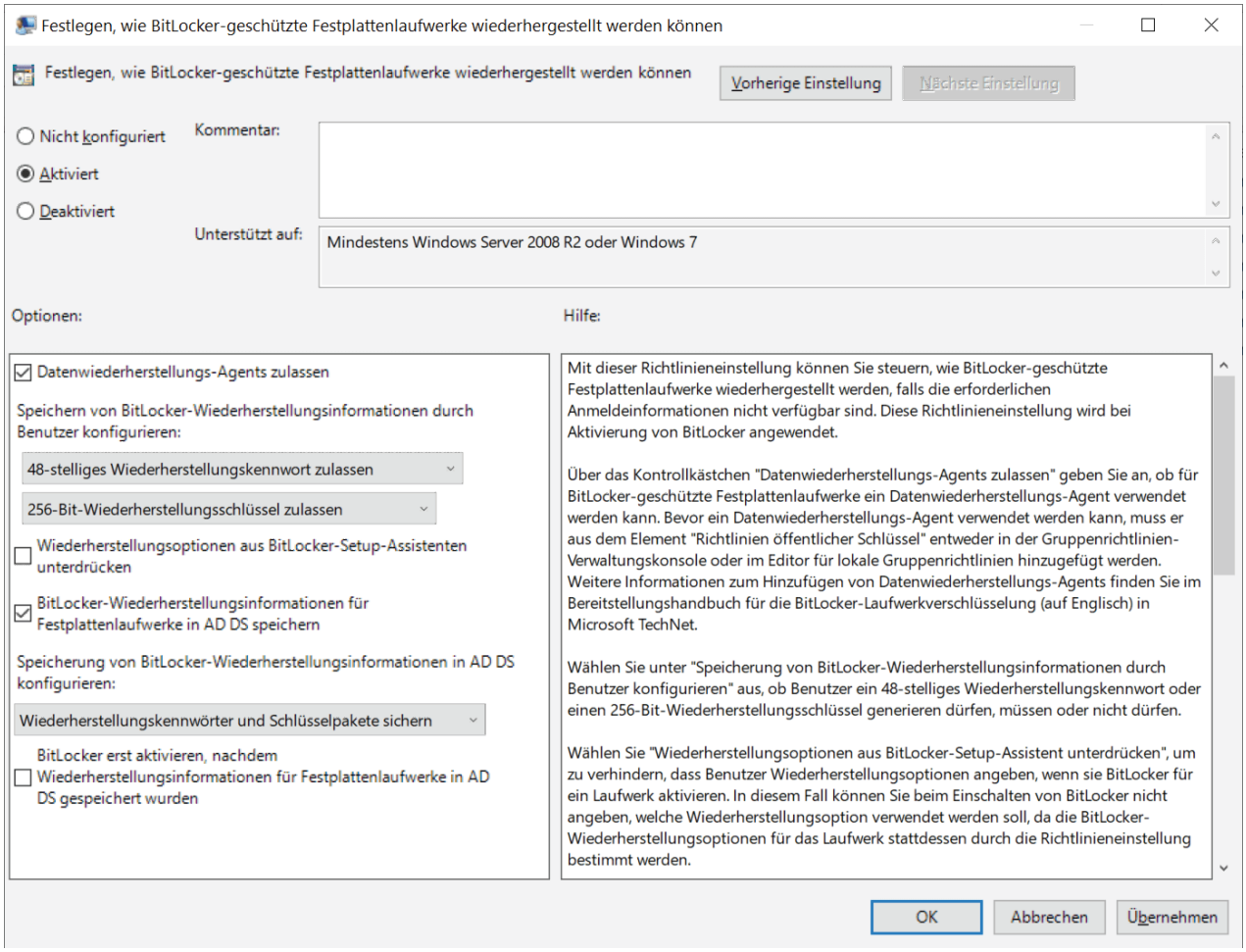
Die Authentifizierung mit TPM und PIN erfordert physischen Zugriff auf den Rechner, wenn er hochfährt oder aus dem Ruhezustand aufwacht. Dies kann ein Hindernis für das Remote-Management sein, bei dem PCs über Wake-on-LAN starten. Für diesen Fall bietet Microsoft die BitLocker Netzwerkentsperrung.

Das Hinzufügen eines Protectors ist hier nur ein kleiner Teil der Konfiguration. Man benötigt dafür ein spezielles Zertifikat, die Windows Deployment Services und einen DHCP-Server.

Protectors verwalten

Microsoft sieht für das Management der Key Protectors ein Zusammenspiel von Gruppenrichtlinien und PowerShell bzw. manage-bde vor. Für alle drei Typen von Datenträgern existiert die GPO-Einstellung *Festlegen, wie BitLocker-geschützte Laufwerke wiederhergestellt werden können.*

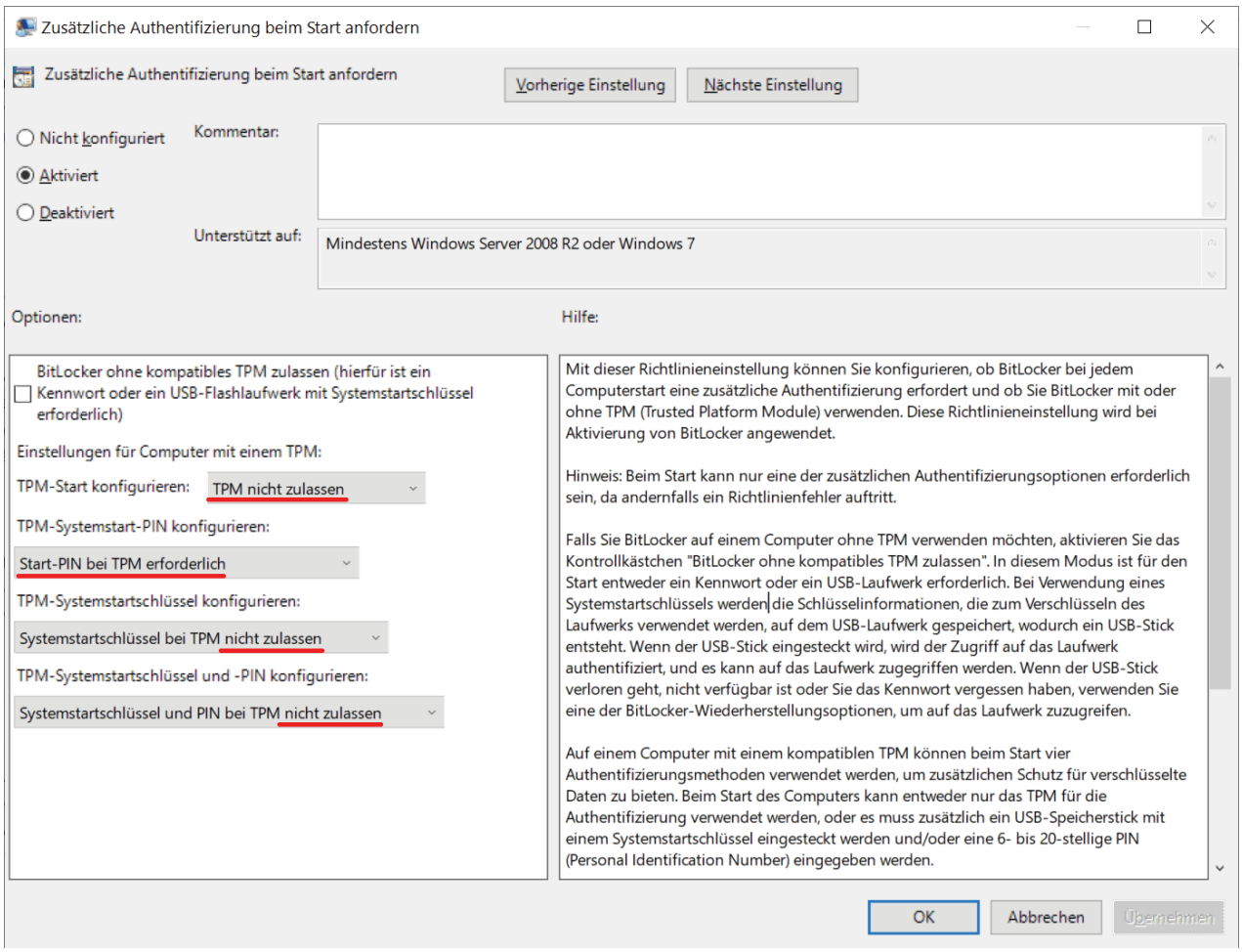
Dort kann man Recovery Agents, Wiederherstellungspasswörter und externe Recovery Keys zulassen, erzwingen oder verbieten.



Gruppenrichtlinie zur Festlegung der zulässigen Protectors für die Wiederherstellung

Für Betriebssystemlaufwerke existieren zusätzlich die Einstellungen Netzwerkentsperrung beim Start zulassen sowie Zusätzliche Authentifizierung beim Start anfordern.

Die erste bezieht sich auf den Network Unlock und die zweite behandelt solche Protectors, die BitLocker für Daten- und Wechsellaufwerke nicht unterstützt. Dies betrifft die Kombinationen aus TPM, PIN und Startup-Schlüssel.



Einstellungen für die TPM-basierte Authentifizierung

Die in den Gruppenrichtlinien vorgenommenen Einstellungen bestimmen das Verhalten des Assistenten zum Aktivieren von BitLocker, den man in der Systemsteuerung findet. Abhängig von den konfigurierten Richtlinien bietet er die blockierten Protectors nicht mehr an oder fordert umgekehrt das Festlegen einer PIN oder eines Passworts, wenn diese genutzt werden müssen.

Die Gruppenrichtlinien blockieren auch das Anlegen von nicht zulässigen Protectors, wenn Benutzer dafür PowerShell oder manage-bde verwenden wollen. Die Group Policies berücksichtigen allerdings nicht alle Protectors, so dass man etwa Auto Unlock oder SID-Protectors damit nicht verhindern kann.

Protector hinzufügen

Bevorzugt man manage-bde für diese Aufgabe, dann sieht ein Aufruf so aus:

manage-bde -protectors -add <Laufwerk:> -<Protector>

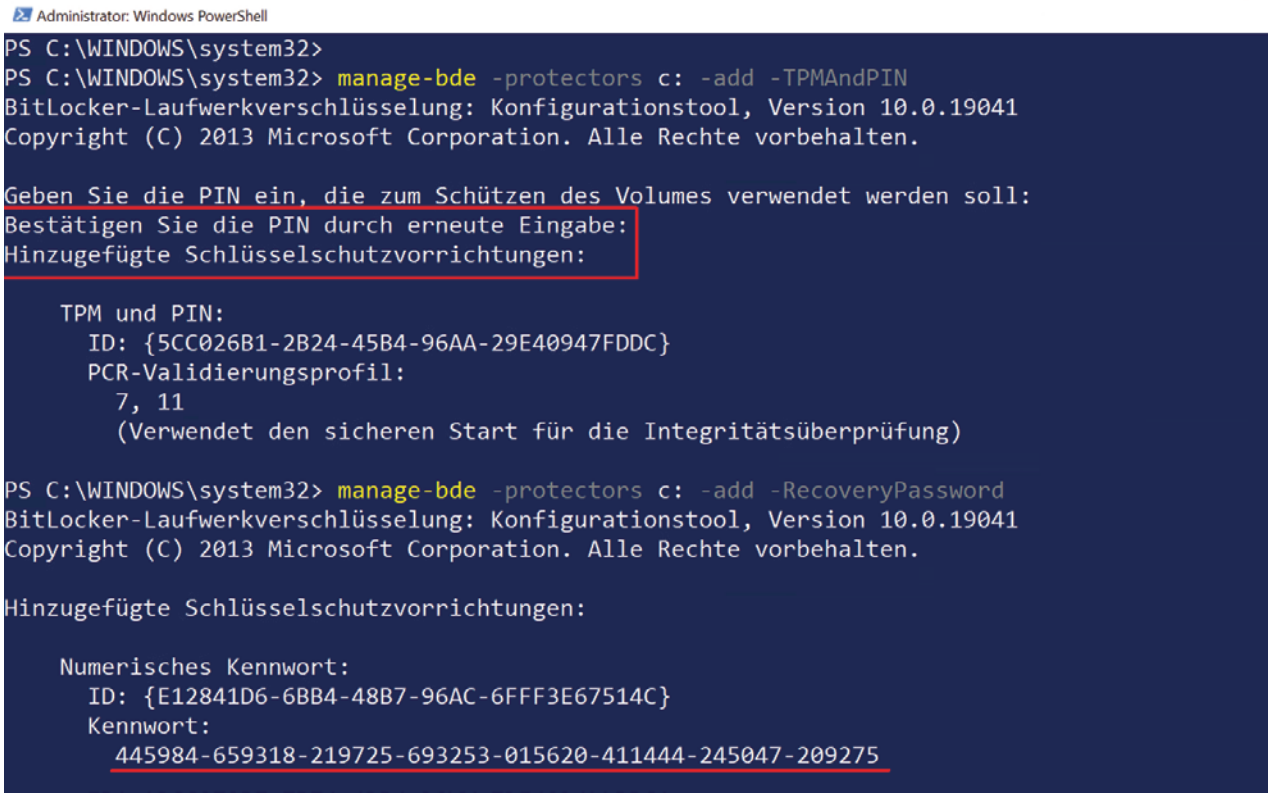
Für <Protector> sind zulässig:

- RecoveryPassword oder -rp
- RecoveryKey oder -rk
- StartupKey oder -sk
- Certificate oder -cert
- TPMAndPIN oder -tp
- TPMAndStartupKey oder -tsk
- TPMAndPINAndStartupKey oder -tpsk
- tpm
- Password oder -pw
- ADAccountOrGroup oder -sid

Zum Beispiel würde das folgende Kommando einen Wiederherstellungsschlüssel für Laufwerk c: erzeugen:

manage-bde -protectors -add c: -RecoveryPassword

Der 48-stellige Key wird dabei automatisch generiert und auf der Konsole angezeigt. Hingegen muss man ein Passwort interaktiv eingeben, das Gleiche gilt für die PIN.

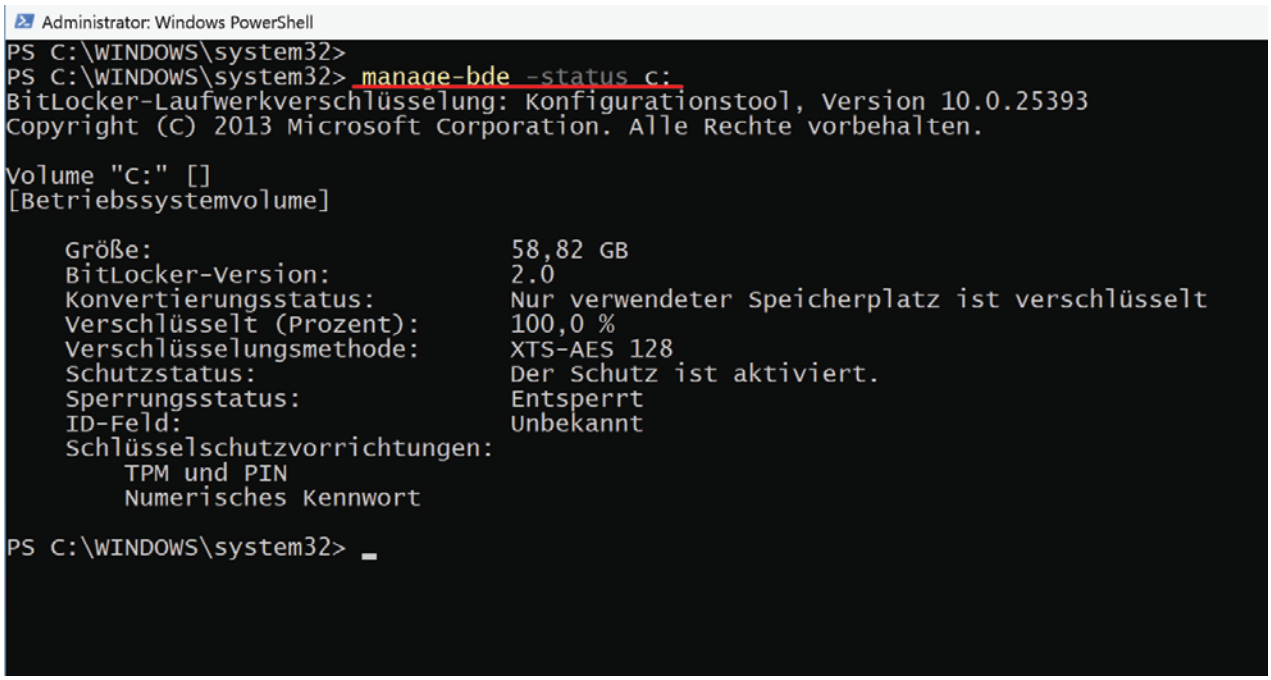


Anlegen von Key Protectors mit manage-bde: Der Recovery Key wird automatisch erzeugt, eine PIN jedoch nicht.

Wenn man den Parameter *ComputerName* bzw. *cn* angibt, dann kann man Protectors auch remote auf anderen PCs verwalten.

Um sich zu überzeugen, welche Protectors für c: existieren, ruft man manage-bde so auf:

manage-bde -status c:

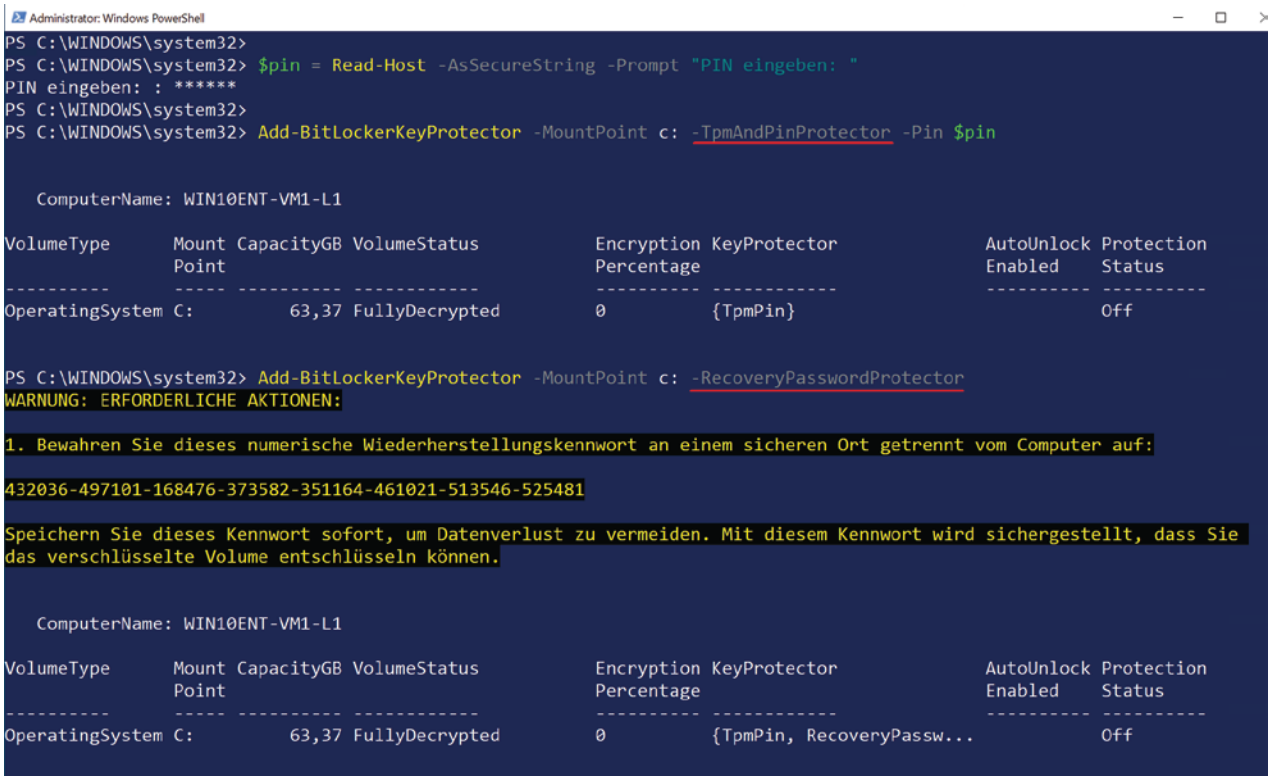


Der von manage-bde angezeigte Status enthält auch eine Übersicht über die konfigurierten Key Protectors

Key Protectors mit PowerShell erstellen

In PowerShell ist das Cmdlet Add-BitLockerKeyProtector für diese Aufgabe zuständig. Man kann ihm Passwörter und PINs als Secure String an die entsprechenden Parameter übergeben, andernfalls werden sie interaktiv abgefragt:

```
$pin = Read-Host -AsSecureString -Prompt "PIN eingeben"
Add-BitLockerKeyProtector -MountPoint c: -TpmAndPinProtector -Pin $pin
```



TPM mit PIN und Wiederherstellungspasswort mit PowerShell anlegen

Wie man sieht, sind die Namen für die Protectors über die verschiedenen Tools hinweg nicht konsistent. Die Parameter für manage-bde und *Add-BitLockerKeyProtector* heißen anders, und bei den WMI-Funktionen muss man sich nochmal umstellen.

Das Cmdlet unterstützt den Parameter *ComputerName* nicht, so dass man für das Management entfernter PCs eine Remote-Session starten müsste.

Um zu prüfen, welche Protectors konfiguriert sind, bietet sich ein solcher Aufruf an:

```
Get-BitLockerVolume -MountPoint "c:" |
select -ExpandProperty KeyProtector
```

Protectors mit WMI hinzufügen

Will man für diese Aufgabe die WMI-Klasse Win32_EncryptableVolume verwenden, dann benötigt man in PowerShell das Cmdlet Get-WmiObject, weil viele Methoden in Get-CimInstance nicht zur Verfügung stehen.

Die obigen Beispiele würde man für einen Remote-PC hiermit so umsetzen:

```
$bl = Get-WmiObject -Namespace "Root\cimv2\security\MicrosoftVolumeEncryption" `
-ClassName Win32_EncryptableVolume -Filter 'DriveLetter="c:"' `
-ComputerName win11-vm1-l1
```

48-stellingen Recovery Key einrichten

$bl.ProtectKeyWithNumericalPassword()

TPM mit PIN, den Wert für die PIN als String mitgeben

$bl.ProtectKeyWithTPMAndPIN("TPMundPIN", "", "123456")

```
Unbenannt1.ps1*  Unbenannt2.ps1*
 1  $bl = Get-WmiObject -Namespace "Root\cimv2\security\MicrosoftVolumeEncryption" `
 2  -ClassName Win32_EncryptableVolume -Filter 'DriveLetter="c:"' `
 3  -ComputerName win10ent-vm1-l1
 4
 5  # 48-stellingen Recovery Key einrichten
 6  $bl.ProtectKeyWithNumericalPassword()
 7
 8  # TPM mit PIN, und den Wert für die PIN als String mitgeben
 9  $bl.ProtectKeyWithTPMAndPIN("TPMundPIN", "", "123456")
10
11  $bl.GetKeyProtectors()
```

```
PS C:\WINDOWS\system32> $bl.GetKeyProtectors()


__GENUS              : 2
__CLASS              : __PARAMETERS
__SUPERCLASS         :
__DYNASTY            : __PARAMETERS
__RELPATH            :
__PROPERTY_COUNT     : 2
__DERIVATION         : {}
__SERVER             :
__NAMESPACE          :
__PATH               :
ReturnValue          : 0
VolumeKeyProtectorID : {{2DDEA952-4CA9-4683-9AA5-62C0CFEC6EBE}, {83DA780C-3159-4D9F-AF36-32643799FE0B}}
PSComputerName       :
```

TPM mit PIN sowie Recovery Key über WMI erzeugen

Die Funktion *ProtectKeyWithNumericalPassword()* generiert zwar das Wiederherstellungs- passwort, gibt es aber nicht aus. Dieses muss man daher separat in Erfahrung bringen, wobei man dazu die ID das Protectors benötigt, die man beim Anlegen angezeigt bekommt:

$bl.GetKeyProtectorNumericalPassword("{6A9BD3E2-373C-4898-9227-A805D38667FE}")

Abschließend kann man mit

$bl.GetKeyProtectors() | select -ExpandProperty VolumeKeyProtectorID

die konfigurierten Protectors anzeigen, wobei man hiermit nur deren ID erhält. Über diese Funktion kann man dann den Typ ermitteln:

$bl.GetKeyProtectorType("{2DDEA952-4CA9-4683-9AA5-62C0CFEC6EBE}")

Das Ergebnis ist numerisch, seine Bedeutung kann man in der Dokumentation nachsehen.

Protector entfernen

Wenn man schließlich Protectors von einem Laufwerk entfernen möchte, dann lässt sich das so erledigen:

```
Remove-BitLockerKeyProtector -MountPoint "c:" `
-KeyProtectorId "{6A2DEFC2-2348-4A5B-9337-F3E2B33B5943}"
```

Die ID des Protectors kann man der Ausgabe von Get-BitLockerVolume entnehmen:

```
Get-BitLockerVolume -MountPoint
```

Bevorzugt man für das Löschen manage-bde.exe, dann sieht der Befehl so aus:

```
manage-bde -protectors -delete C: -id {6A2DEFC2-2348-4A5B-9337-F3E2B33B5943}
```

Alternativ kann man alle Key Protectors eines Typs so entfernen:

```
manage-bde -protectors -delete c: -Type RecoveryPassword
```

Systemintegrität mittels PCR-Profil validieren

Ein vertrauenswürdiger PC, dessen Komponenten nicht manipuliert wurden, ist eine wichtige Bedingung dafür, dass der Schutz von BitLocker nicht unterlaufen werden kann. Das gilt besonders dann, wenn aus Gründen der Benutzerfreundlichkeit nur ein TPM-Protector konfiguriert wurde.

In dieser Situation muss sichergestellt sein, dass das TPM den Full Volume Encryption Key nur entschlüsselt, wenn die Integrität des Systems gewährleistet ist. Zu diesem Zweck sichert BitLocker mit den in den Platform Configuration Register (PCR) des TPM gespeicherten Daten den kompletten Boot-Vorgang von der Firmware bis zum Betriebssystem ab.

Die hier beschriebenen Einstellungen gelten nur für Rechner mit TPM. Ist ein solcher nicht vorhanden, lässt sich die Vertrauenswürdigkeit des Systems nicht validieren. In diesem Fall ist aber ohnehin der Einsatz eines zusätzlichen Protectors erforderlich.

Hier sind die englischen Beschreibungen der Register, nachdem Microsofts deutsche Übersetzung der PCR-Dokumentation unvollständig und irreführend ist:

- PCR 0: Core root-of-trust for measurement, EFI boot and run-time services, EFI drivers embedded in system ROM, ACPI static tables, embedded SMM code, and BIOS code
- PCR 1: Platform and motherboard configuration and data. Hand-off tables and EFI variables that affect system configuration
- PCR 2: Option ROM code
- PCR 3: Option ROM data and configuration
- PCR 4: Master Boot Record (MBR) code or code from other boot devices
- PCR 5: Master Boot Record (MBR) partition table. Various EFI variables and the GPT table
- PCR 6: State transition and wake events
- PCR 7: Computer manufacturer-specific
- PCR 8: NTFS boot sector
- PCR 9: NTFS boot block
- PCR 10: Boot manager
- PCR 11: BitLocker access control

Es liegt auf der Hand, dass diese Prüfung umso leichter scheitern kann, je mehr Kriterien erfüllt sein müssen, um einen PC als vertrauenswürdig gelten zu lassen.

PCR für die Absicherung des Systemstarts

Entdeckt BitLocker Abweichungen am System gegenüber dem ursprünglichen Zustand, dann zeigt er die so genannte Wiederherstellungskonsole an und erwartet vom Benutzer die Eingabe des Recovery Key.

Nach dessen Eingabe entsperrt BitLocker das betreffende Laufwerk und setzt das Validierungsprofil zurück, damit beim nächsten Start nicht wieder die Recovery-Konsole erscheint. Dies kann man bei Bedarf verhindern, indem man die Gruppenrichtlinie *Plattformvalidierungsdaten nach BitLocker-Wiederherstellung zurücksetzen aktiviert*.

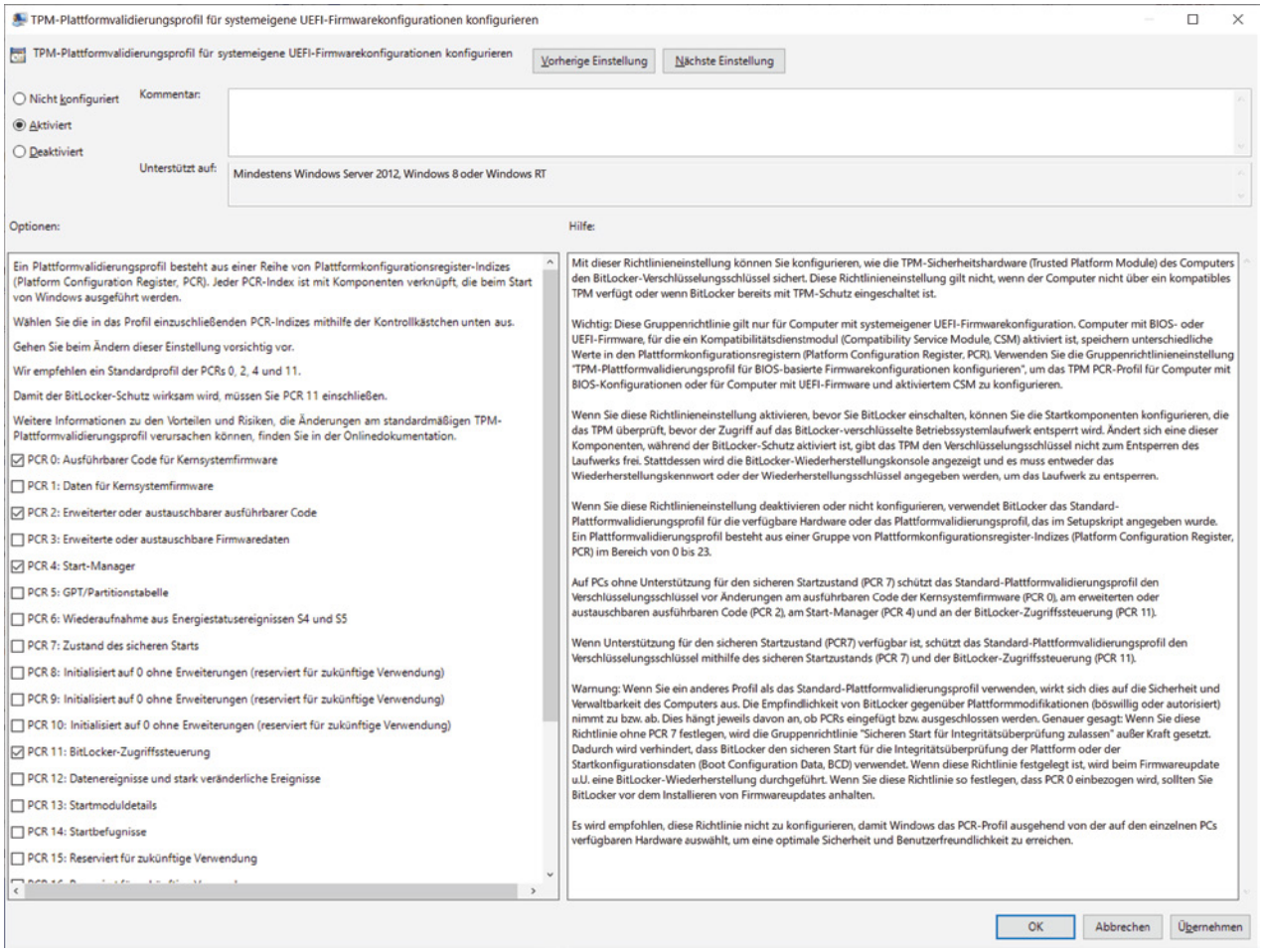
Das Entsperren mit Hilfe des Recovery Key führt in der Regel zu einer Anfrage beim Helpdesk. Arbeiten viele Mitarbeiter eines Unternehmens von unterwegs mit ihren Notebooks, dann kann es einigen Aufwand erzeugen, die Benutzer verlässlich zu identifizieren und den Schlüssel sicher zu übertragen.
Aus diesem Grund kann es sinnvoll sein, die von BitLocker verwendeten PCR anzupassen. Für diesen Zweck bieten die Gruppenrichtlinien eine entsprechende Einstellung.

Validierungsprofil anpassen

Sie findet sich unter *Computerkonfiguration => Richtlinien => Administrative Vorlagen => Windows-Komponenten => BitLocker Laufwerksverschlüsselung => Betriebssystemlaufwerke* und existiert in drei Ausprägungen:

- TPM-Plattformvalidierungsprofil für systemeigene UEFI-Firmwarekonfigurationen konfigurieren ("Configure TPM platform validation profile for native UEFI firmware configurations")
- TPM-Plattformvalidierungsprofil für BIOS-basierte Firmwarekonfigurationen konfigurieren ("Configure TPM platform validation profile for BIOS-based firmware configurations")
- PM-Plattformvalidierungsprofil konfigurieren (Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2) ("Configure TPM platform validation profile (Windows Vista Windows Server 2008 Windows 7 Windows Server 2008 R2"))

Die letzten beiden dürften in den meisten Umgebungen keine Rolle mehr spielen, wenn UEFI-Rechner mit einem zeitgemäßen Windows eingesetzt werden.



Gruppenrichtlinie zur Konfiguration des Profils zur TPM-Plattformvalidierung

Auf BIOS-Rechnern sind standardmäßig PCR 0, 2, 4, 8, 9, 10 und 11 aktiviert, auf UEFI-PCs mit aktiviertem Secure Boot nur PCR 7 und 11. Mit PCR 7 übernimmt Secure Boot einen Großteil der Validierung und ersetzt somit PCR 0, 2 und 4.

Der größte Bedarf für Anpassungen besteht also auf BIOS-PCs sowie auf UEFI-Rechnern, wenn Secure Boot nicht erwünscht oder nicht möglich ist, etwa weil wegen einer bestimmten Hardware-Komponente das UEFI-Kompatibilitätsmodul aktiviert ist.

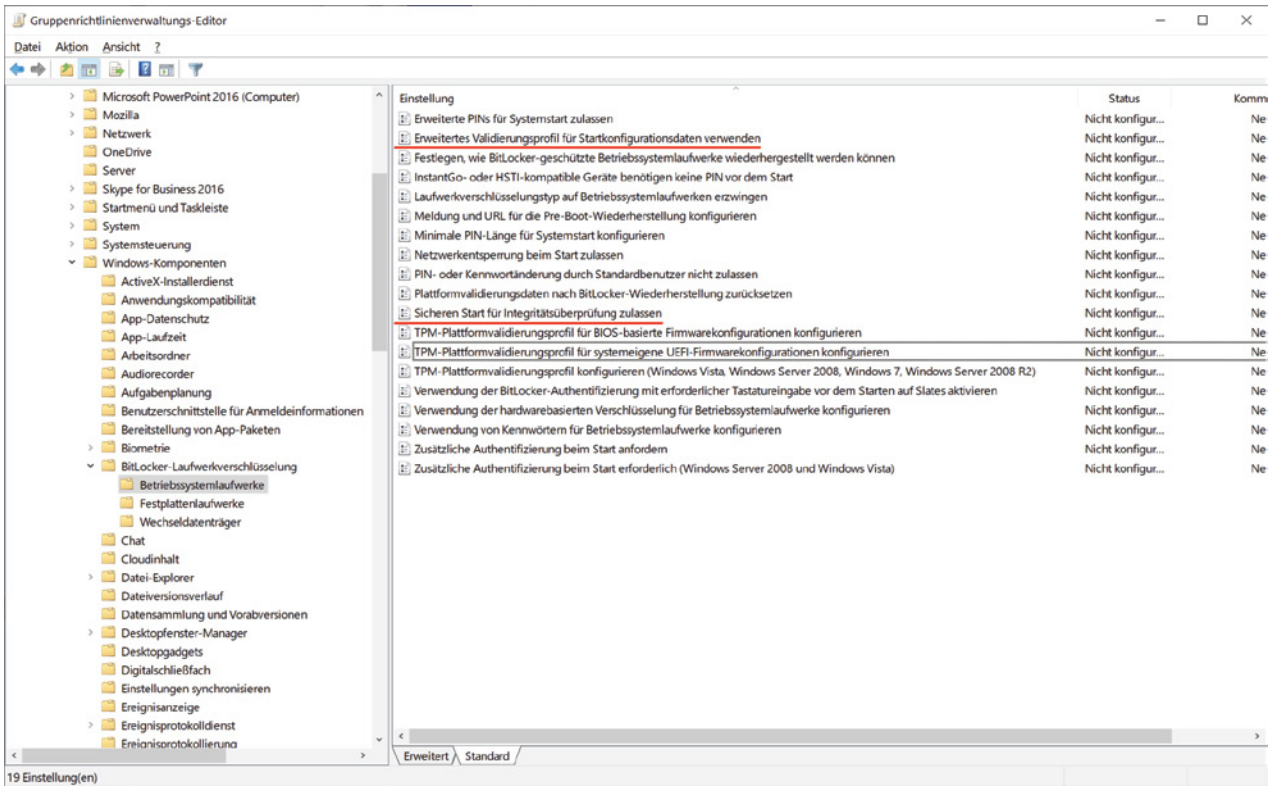
In diesem Fall erweisen sich PCR 2 und 4 als Kandidaten, die sehr schnell den Recovery Mode auslösen können. Die Änderung der Boot-Reihenfolge von Laufwerken reicht dabei schon aus.
Wurde die Windows-Partition verschlüsselt, nachdem der Rechner von einem PXE-Server aus gestartet wurde, dann muss selbst dieser künftig immer verfügbar sein, um die Eingabe des Wiederherstellungs-passworts zu vermeiden.

Hier kann es hilfreich sein, BitLocker zu veranlassen, bestimmte BCD-Einträge zu ignorieren. Zuständig dafür ist die Einstellung *Erweitertes Validierungsprofil für Startkonfigurationsdaten verwenden* ("Use enhanced Boot Configuration Data validation profile").

Die Syntax für BCD-Einstellungen, die zusätzlich überprüft oder ausgeschlossen werden sollen, beschreibt diese Seite der Microsoft-Dokumentation.

Rivalisierende Einstellungen

Wenn man die Einstellung *Sicheren Start für Integritätsprüfung zulassen* aktiviert hat und gleichzeitig das TPM-Plattformvalidierungsprofil mit Hilfe einer der oben genannten Gruppenrichtlinien anpassen möchte, dann sollte man darauf achten, dass dort PCR 7 ausgewählt ist. Andernfalls überschreibt man damit die Einstellung für den sicheren Start.



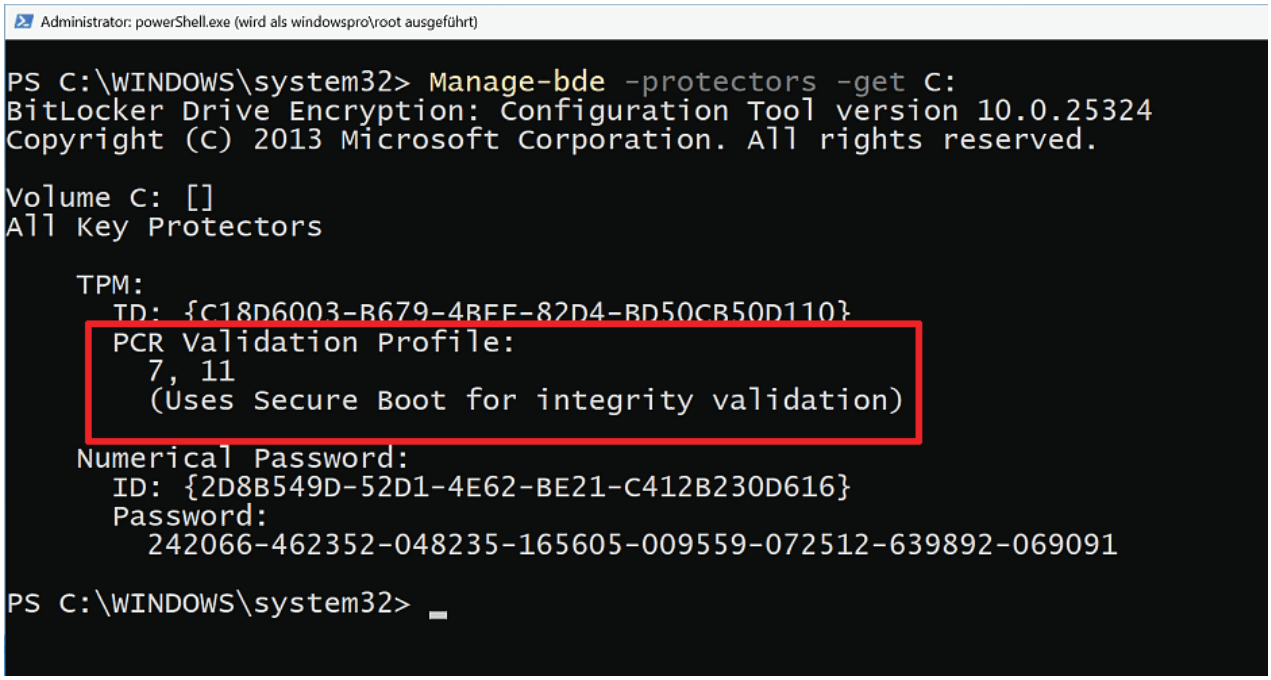
Gruppenrichtlinien, die durch eine konkurrierende Einstellung überschrieben werden können

Nutzt man Secure Boot zur Verifizierung der Systemintegrität, dann wird die erwähnte Einstellung zur Prüfung der BCD-Einträge ignoriert.

Status abfragen

Um herauszufinden, welche PCRs BitLocker aktuell für die Validierung der Systemintegrität verwendet, nutzt man das Dienstprogramm manage-bde.exe:

```
manage-bde -protectors -get %systemdrive%
```

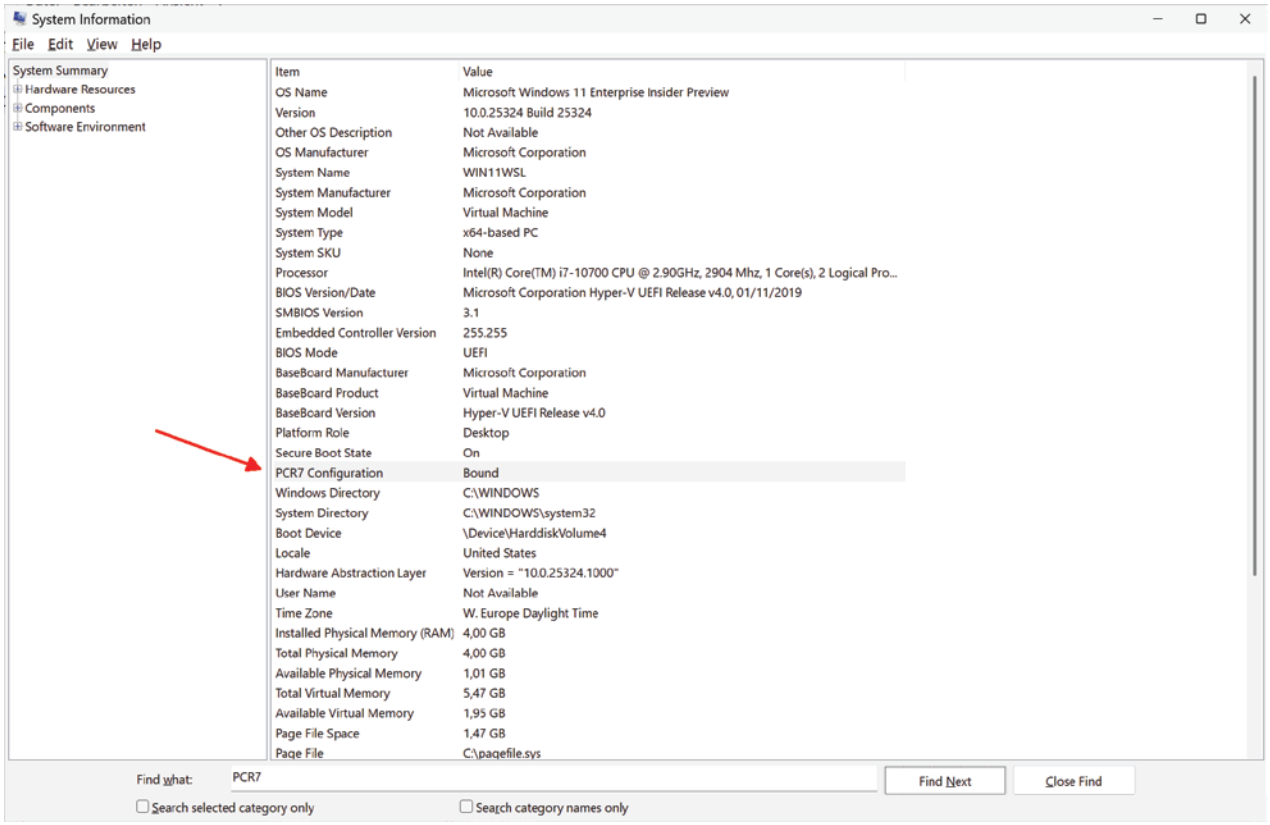


Mit manage-bde anzeigen, welche PCRs für die Systemvalidierung verwendet werden

Die PowerShell-Cmdlets des BitLocker-Moduls sind hierbei nicht hilfreich. Man müsste die entsprechenden Infos stattdessen über WMI abrufen, was *Get-BitLockerVolume* hinter den Kulissen *mit Invoke-CimMethod* ohnehin macht, allerdings ohne Auskunft über die PCRs einzuholen.

Die Systeminformationen (msinfo32.exe) enthalten Informationen zu PCR7, und zwar nur, ob BitLocker an Secure Boot gebunden ist oder nicht.

Ruft man das Tool als Standardbenutzer auf, dann steht unter *PCR7-Konfiguration* "Erweiterung zum Anzeigen erforderlich". Dies ist eine minderwertige Übersetzung von "Elevation Required to View". Man braucht mithin erhöhte Rechte, um diesen Eintrag zu sehen.



Status der PCR7-Konfiguration mit msinfo32 ausgeben

Empfohlenes Vorgehen

BitLocker verwendet eine relativ komplexe Kombination aus verschiedenen Kriterien, um ein System als vertrauenswürdig einzustufen und den Schlüssel aus dem TPM freizugeben. Die benutzerfreundlichste Variante besteht auf moderner Hardware aus PCR 7 und 11.

Secure Boot gewährleistet dabei die Integrität der meisten Komponenten. Es reagiert flexibel auf einige Systemänderungen, beispielsweise nach Updates im BCD-Speicher, und erspart den Benutzern so die Eingabe des Recovery Key.

Unterstützt die Hardware nicht das sichere Booten oder ist dieses wegen möglicher Komplikationen nicht erwünscht, dann ist es sinnvoll, das Validierungsprofil zu optimieren. Damit lässt sich die Häufigkeit des Recovery Mode reduzieren.

BitLocker-Key mit PIN absichern

Auf modernen Rechnern ist BitLocker standardmäßig so konfiguriert, dass das TPM alleine den Volume Master Key (VMK) freigibt. Fällt ein Notebook jedoch in die falschen Hände, dann ist der VMK damit nicht ausreichend geschützt. Daher empfiehlt Microsoft eine Zwei-Faktor-Authentifizierung durch eine zusätzliche PIN oder einen Startup-Key.

Wenn BitLocker das TPM als einzigen Protektor beim Systemstart verwendet, dann ist das die komfortabelste Variante für die Benutzer. Sie erhalten dabei automatisch Zugang zu verschlüsselten Laufwerken.

Volume Master Key angreifbar

Das TPM enthält den Storage Root Key und entschlüsselt damit den VMK. Diesen gibt es allerdings nur dann frei, wenn die Prüfung des Validierungsprofils erweist, dass sich die Systemkonfiguration nicht geändert hat.

Das von BitLocker entsperrte Laufwerk ist dann bereits zugänglich, bevor der Benutzer den Anmeldebildschirm zu sehen bekommt. Der VMK befindet sich mithin unverschlüsselt im RAM des Rechners, von wo ihn ein Angreifer über einen Speicher-Dump auslesen könnte.

Weitere Angriffsvektoren ergeben sich durch Schwachstellen wie CVE-2022-41099, bei der sich die BitLocker-Verschlüsselung des Betriebssystemlaufwerks über WinRE aushebeln lässt.

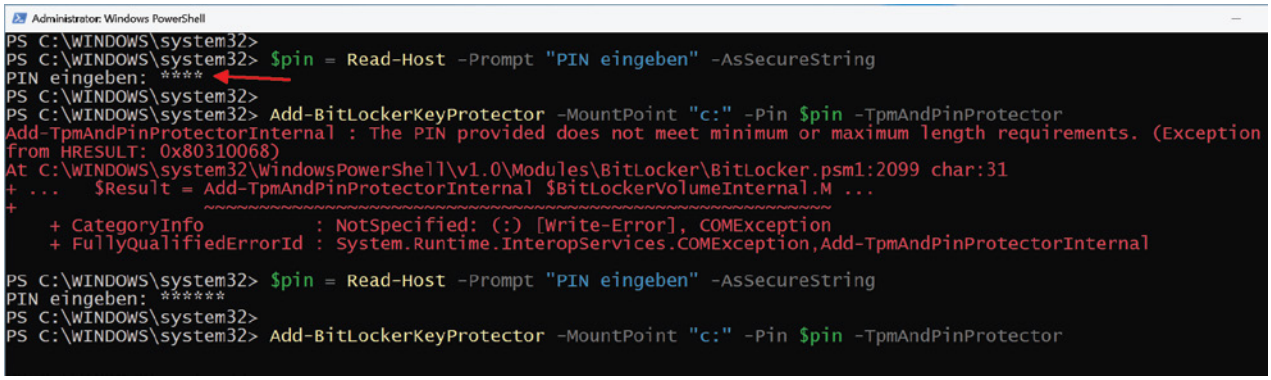
Zweiter Faktor als Schutz gegen VMK-Diebstahl

In solchen Fällen bieten eine PIN oder ein Systemstartschlüssel einen zusätzlichen Schutz, weil sie eine Authentifizierung noch vor dem Booten des Betriebssystems erfordern. Erhält ein Angreifer physischen Zugang zum Rechner, dann scheitert der Angriff mittels Speicher-Dump, weil ohne Eingabe der PIN oder den Start-Key der VMK erst gar nicht entschlüsselt wird.

PIN und Startup-Schlüssel lassen sich entweder einzeln oder zusammen mit dem TPM-Protector kombinieren. Nachdem der Key eine Hardware in Form eines USB-Sticks erfordert, bevorzugen die meisten Anwender den komfortableren Einsatz einer PIN.

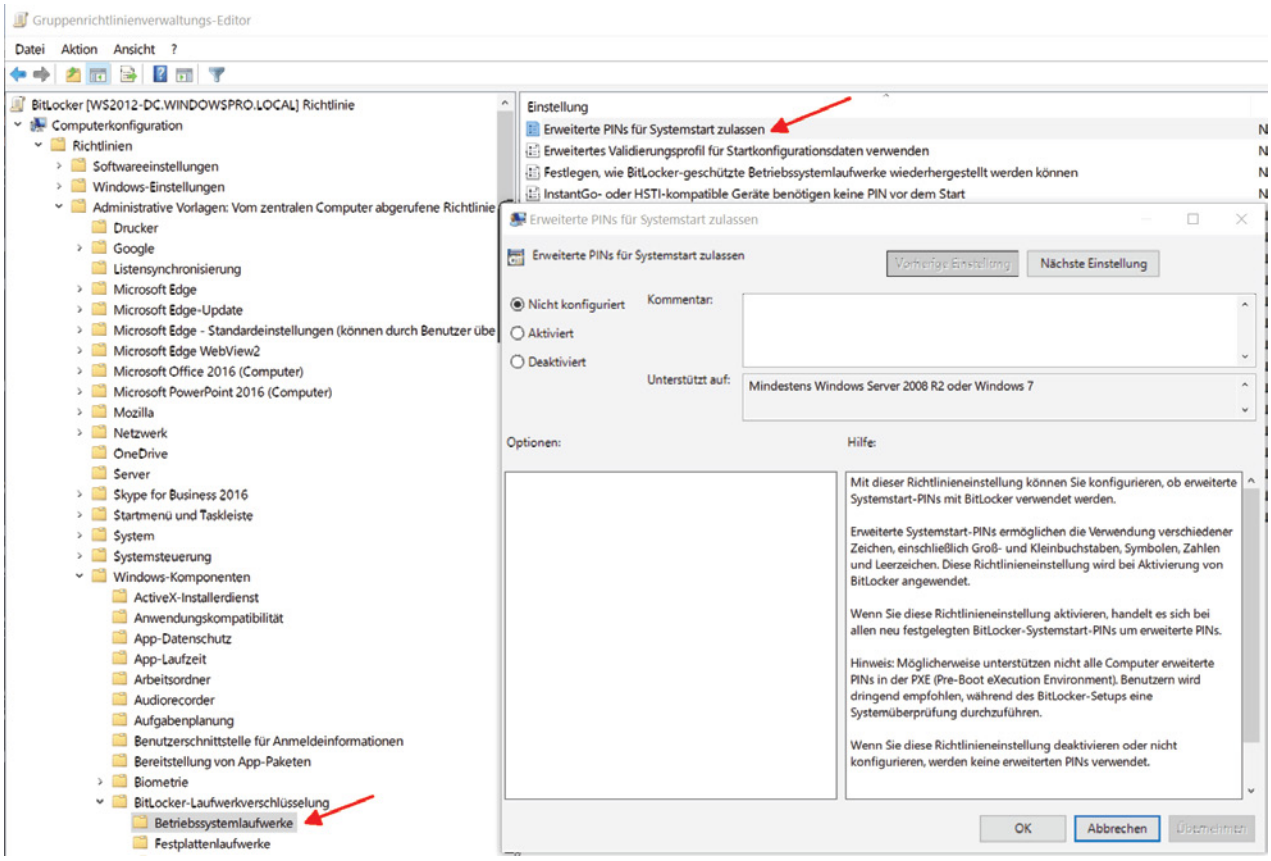
PIN-Sperre nach Fehlversuchen

Das TPM schützt die PIN gegen Brute-Force-Angriffe, indem es nach mehreren (in der Regel 32) Fehleingaben den Zugang sperrt und dann nur alle 10 Minuten einen weiteren Versuch zulässt. Microsoft hat zudem die Hürde für solche Attacken höher gelegt, indem die Mindestlänge nun standardmäßig 6 und nicht mehr wie früher 4 Zeichen beträgt.



Der Versuch, einen Protector mit einer vierstelligen PIN einzurichten, scheitert auf neueren Windows-Versionen

Darüber hinaus kann man mit der Gruppenrichtlinie *Erweitere PINs für Systemstart zulassen* ("Allow enhanced PINs at startup") dafür sorgen, das Benutzer auch komplexere PINs verwenden dürfen, die neben Ziffern auch Buchstaben und andere Zeichen enthalten.



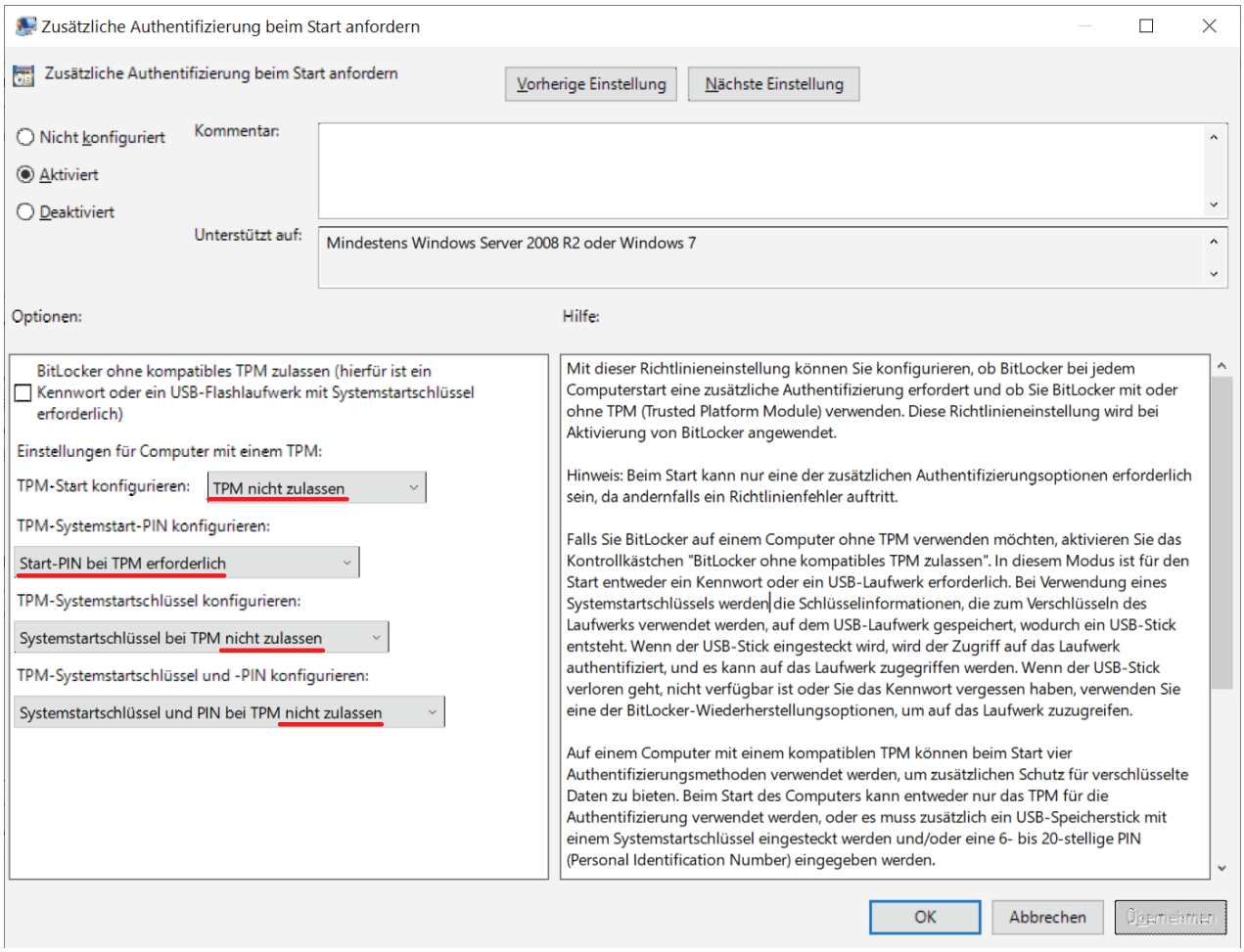
Komplexe PINs mittels Gruppenrichtlinie erlauben

Allerdings sollte man beachten, dass es dabei zu Problemen der Tastaturbelegung kommen kann. Während beim Festlegen der PIN noch das deutsche Layout gilt, erfolgt die Abfrage der PIN mit der englischen Belegung. Enthält die erweiterte PIN etwa ein 'z', dann muss der Benutzer ein 'y' eingeben.

Authentifizierungsmethoden vor BitLocker-Aktivierung festlegen

Wenn man die Verfahren zur Authentifizierung oder zur Wiederherstellung von verschlüsselten Laufwerken mittels Gruppenrichtlinien konfigurieren möchte, dann sollte man dies vor der Aktivierung von BitLocker tun.

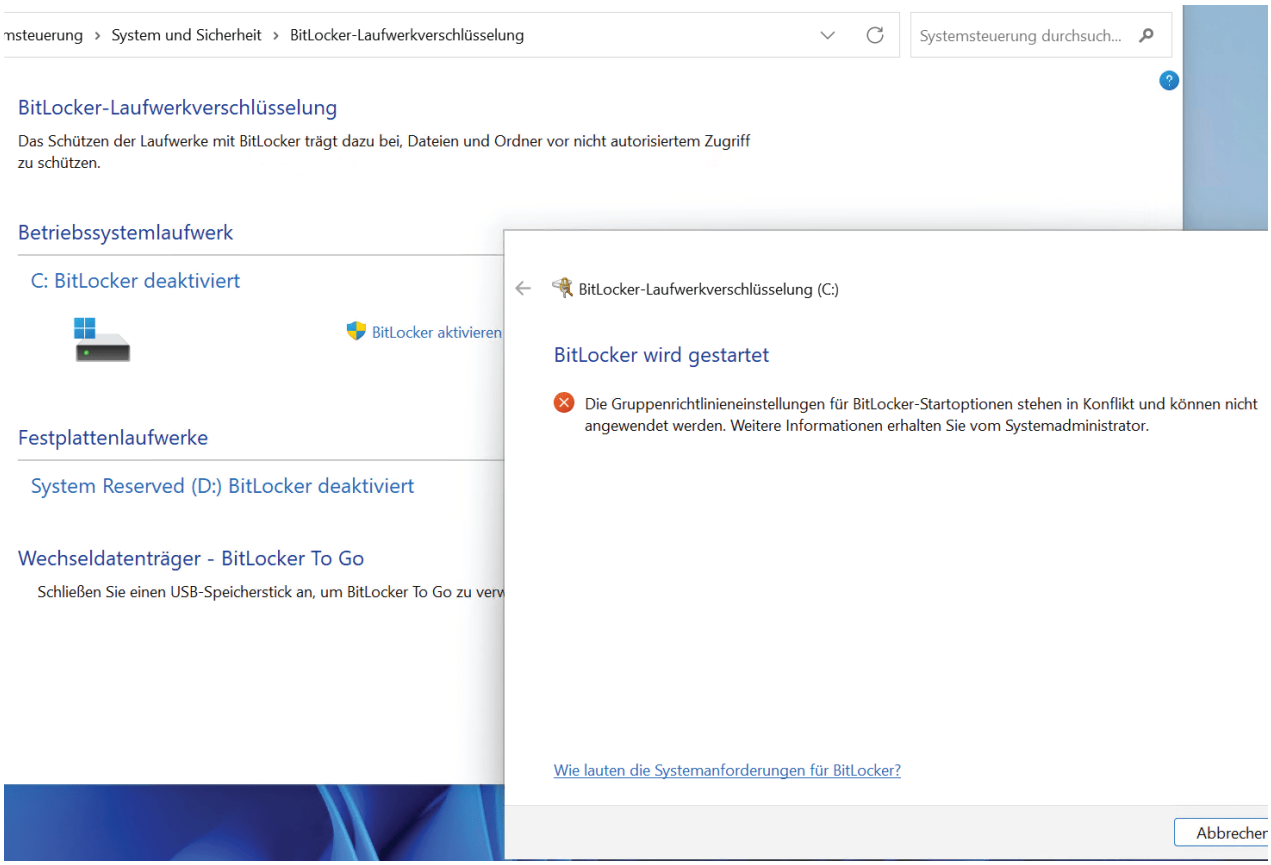
Zuständig ist dafür die Einstellung *Zusätzliche Authentifizierung beim Start anfordern* ("Require additional authentication at startup"). Sie findet sich unter *Computerkonfiguration => Richtlinien => Administrative Vorlagen => Windows-Komponenten => BitLocker-Laufwerksverschlüsselung => Betriebssystemlaufwerke.*



Nur eine der zusätzlichen Methoden darf vorgegeben werden

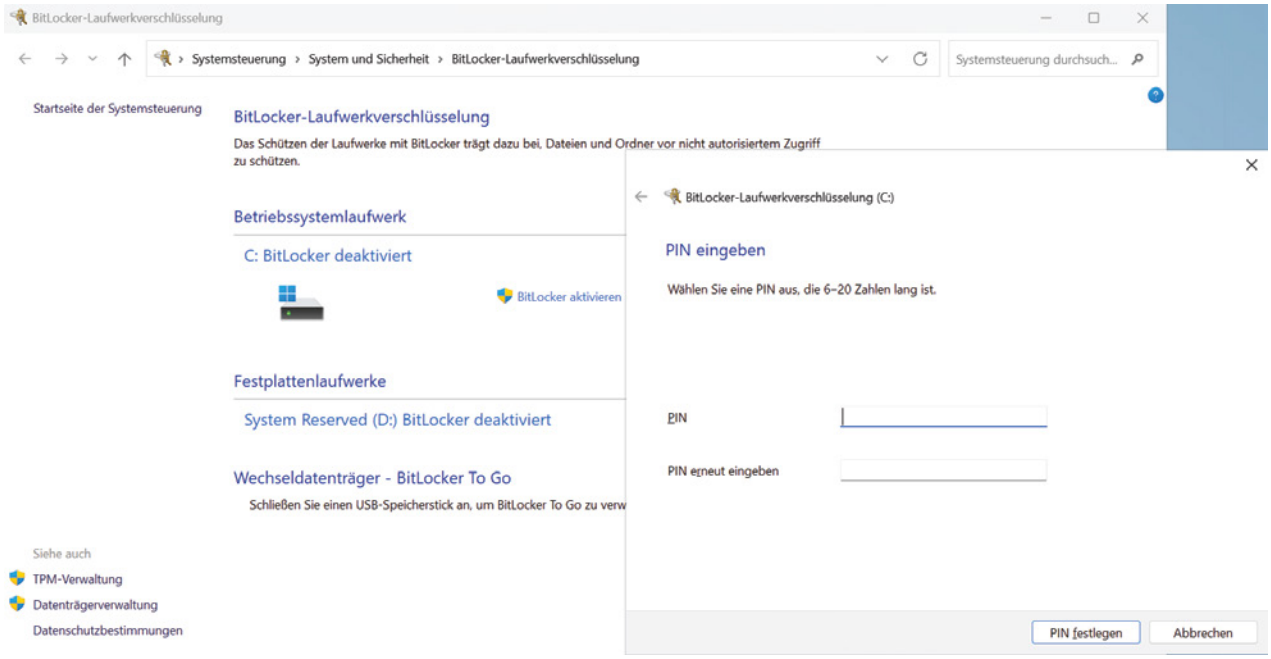
Hier ist zu beachten, dass man unter *Einstellungen für Computer mit einem TPM* nur eine Option als erforderlich festlegen darf. Alle anderen muss man auf *nicht zulassen* setzen, darunter auch *TPM-Start konfigurieren,* wenn man eine PIN verwenden will. Andernfalls gibt der Assistent zum Aktivieren von BitLocker folgende Fehlermeldung aus:

"Die Gruppenrichtlinien für die BitLocker-Startoptionen stehen in Konflikt und können nicht angewendet werden."



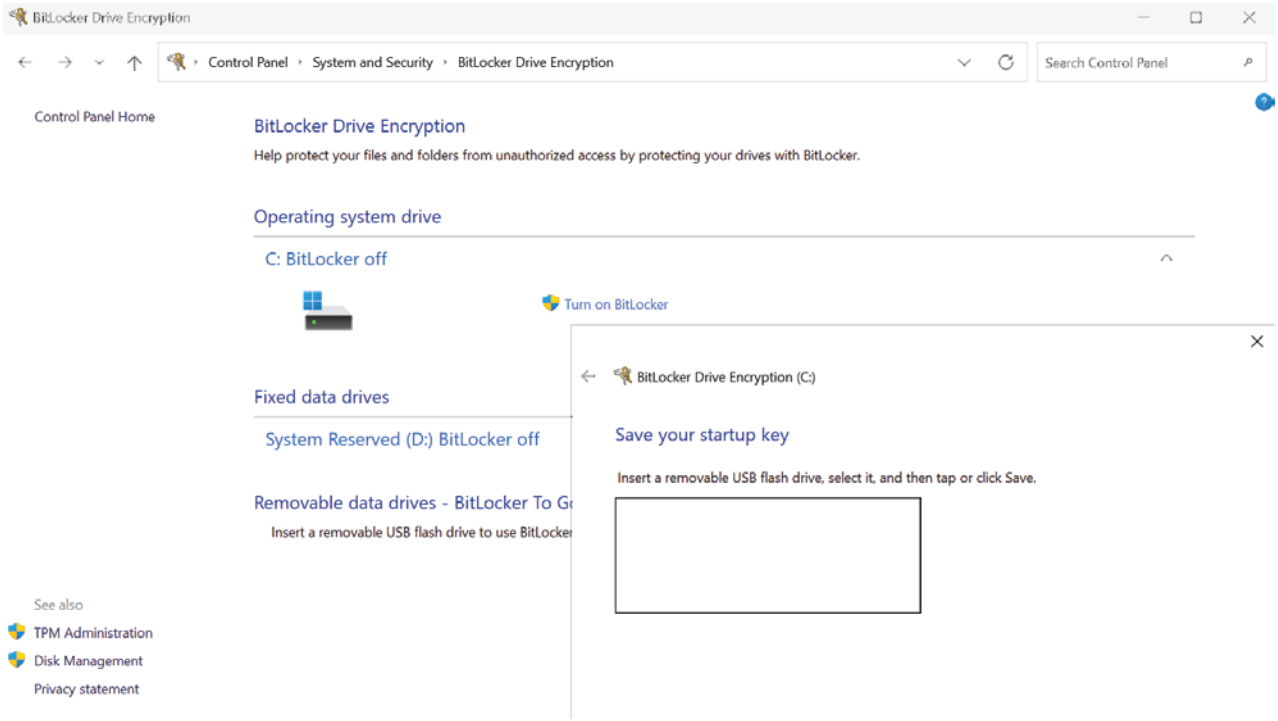
Fehlermeldung im BitLocker-Assistenten, wenn per GPO mehrere Startoptionen konfiguriert sind

Wenn dazu berechtigte Benutzer nach der korrekten Konfiguration der Gruppenrichtlinie BitLocker einschalten, dann fordert der Assistent aus der Systemsteuerung die Daten für die im GPO definierten Protektoren an. Das ist im Fall von TPM und PIN ein mindestens sechsstelliger numerischer Code.



Wenn man über Gruppenrichtlinien eine Start-PIN konfiguriert hat,
dann muss man diese beim Aktivieren von BitLocker festlegen

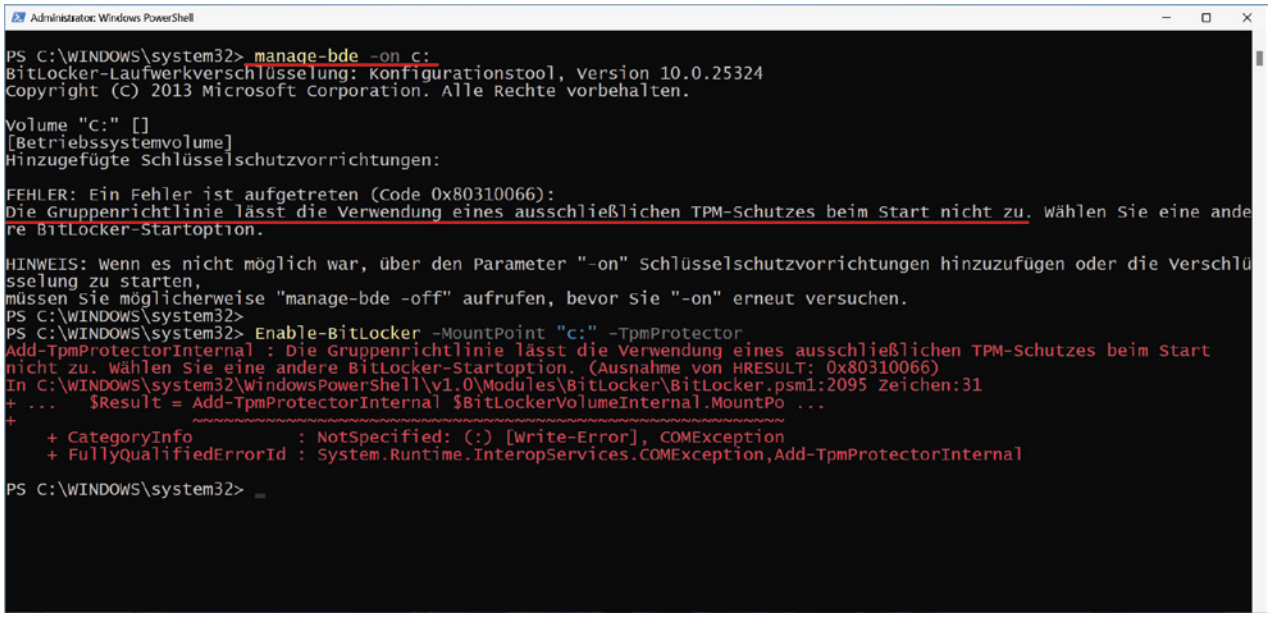
Hat man sich alternativ oder zusätzlich für den Einsatz eines Startschlüssels entschieden, dann verlangt der Assistent die Bereitstellung bzw. die Auswahl eines USB-Sticks.



Verlangt die Gruppenrichtlinie die Verwendung eines Startup-Keys,
dann muss man bei der BitLocker-Aktivierung einen USB-Stick bereitstellen

BitLocker mittels PowerShell oder manage-bde aktivieren

Möchte man BitLocker stattdessen über die Kommandozeile, also mit PowerShell oder manage-bde.exe aktivieren, dann kann man nur jene Protektoren angeben, die im GPO konfiguriert sind. Andernfalls läuft man in eine Fehlermeldung.



Beim Aktivieren von BitLocker über die Kommandozeile muss man sich an die Vorgaben durch das GPO halten

PIN nachträglich hinzufügen

Hat man BitLocker auf dem Betriebssystemlaufwerk bereits einschaltet und mit dem standardmäßigen TPM-Protektor versehen, dann bewirkt eine Änderung in der oben beschriebenen GPO-Einstellung per se kein Anlegen des TPMAndPIN-Protectors.

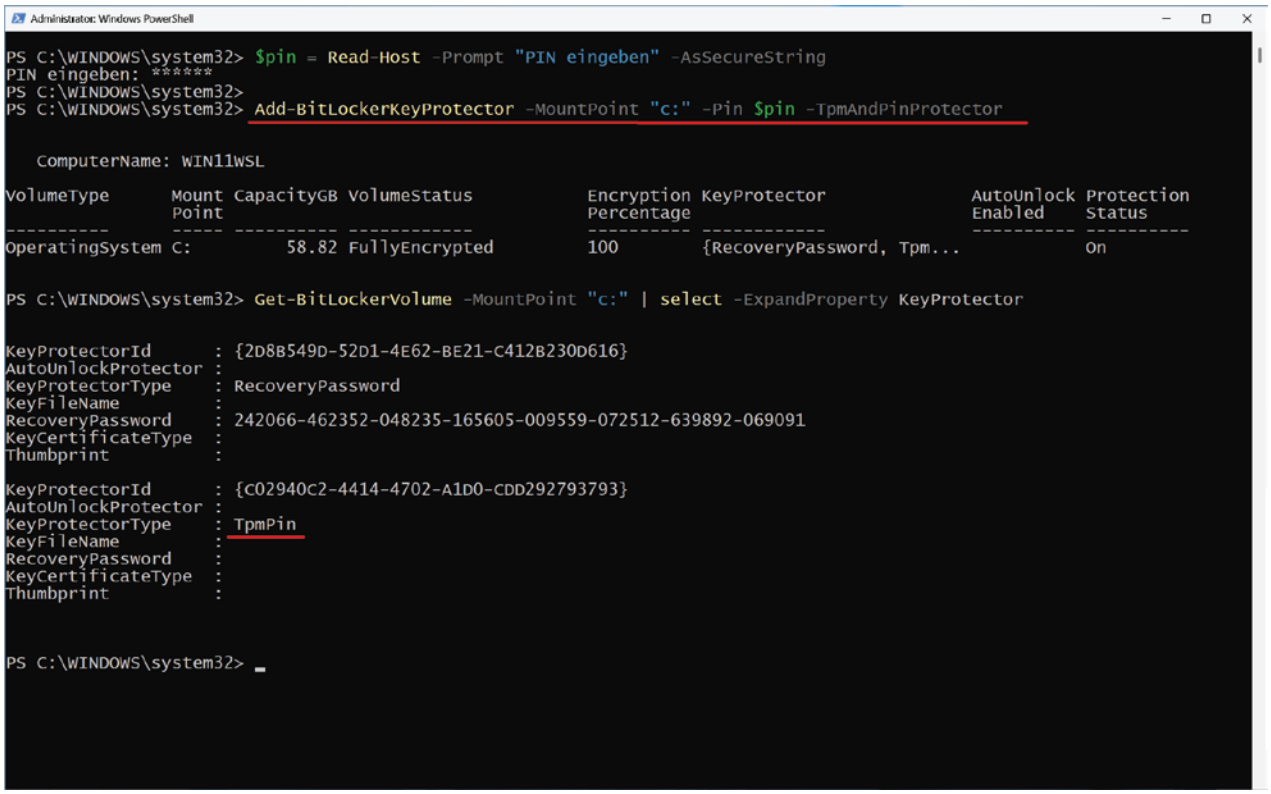
In diesem Fall kann man aber einen weiteren Protektor mittels PowerShell oder manage-bde hinzufügen:

manage-bde -protectors -add c: -TPMAndPIN

Mit PowerShell würde man so vorgehen:

$pin = Read-Host -Prompt "PIN eingeben" -AsSecureString
Add-BitLockerKeyProtector -MountPoint "c:" -TpmAndPinProtector -Pin $pin

Aber auch hier ist beachten, dass man auf diesem Weg nur Protectors anlegen kann, die nicht im Widerspruch zur zugewiesenen Gruppenrichtlinie stehen.



BitLocker-Protector für TPM und PIN mit PowerShell erzeugen

Es ist insgesamt eine gute und von Microsoft empfohlene Praxis, die implizite Authentifizierung mittels TPM um eine PIN zu ergänzen, die bereits vor dem Booten des Betriebssystems abgefragt wird.

Der Assistent aus der Systemsteuerung richtet die PIN-Authentifizierung nur dann ein, wenn man dem Rechner ein entsprechendes GPO vor dem Aktivieren von BitLocker zugewiesen hat.

Auf der Kommandozeile kann man indes jederzeit einen neuen Protector hinzufügen. Dieser muss aber in den Gruppenrichtlinien konfiguriert sein, ansonsten scheitert die Operation.

BitLocker Recovery Keys im Active Directory speichern

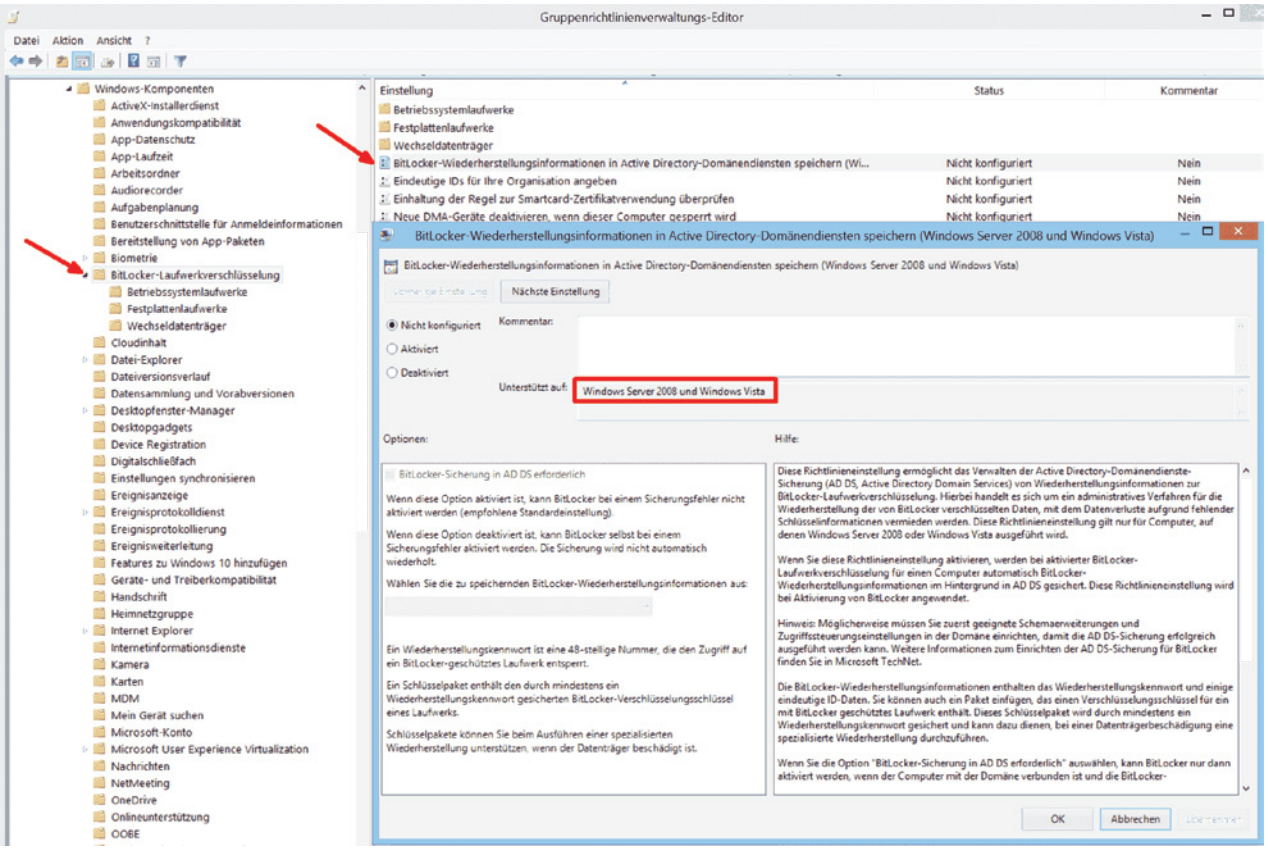
Wenn sich User aus ihrem Rechner aussperren, etwa weil sie PIN vergessen haben oder unerwartet die Wiederherstellungskonsole erscheint, dann hilft nur noch der Recovery Key.

Während private User diesen 48-stelligen Schlüssel ausdrucken, in einer Datei oder im Microsoft-Konto speichern, dient im professionellen Umfeld das Active Directory als bevorzugter Ablageort. Damit ist der Wiederherstellungsschlüssel an einem zentralen Ort abrufbar und vor dem unbefugten Zugriff geschützt. Die sichere Verwaltung des Schlüssels ist somit ohne Tools von Drittherstellern möglich.

Gruppenrichtlinien konfigurieren

Im ersten Schritt erstellt man ein GPO für jene OUs oder Domänen, für deren Computer-Objekte der Recovery Key im Active Directory gespeichert werden soll.

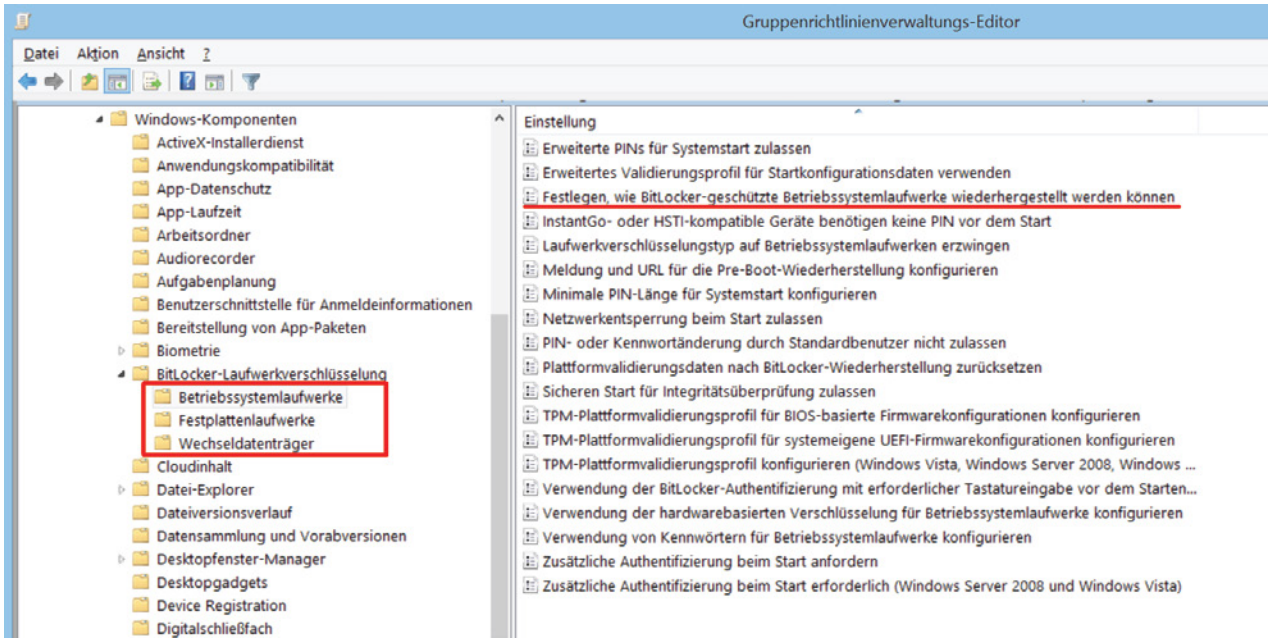
Die Einstellungen für BitLocker finden sich unter *Computerkonfiguration => Administrative Vorlagen => Windows Komponenten => BitLocker-Laufwerksverschlüsselung*. Hier gibt es den Eintrag *BitLocker-Wiederherstellungsinformationen im Active Directory Domaindiensten speichern*. Dieser greift aber nur für Rechner unter Vista und Server 2008, so dass er für die meisten Umgebungen irrelevant sein wird.



Diese Einstellung wirkt nur auf Computer mit Vista oder Windows Server 2008

Neuere Betriebssysteme erlauben eine granulare Konfiguration abhängig von den Laufwerkstypen. BitLocker unterscheidet dabei zwischen Betriebssystem- und Festplattenlaufwerken sowie Wechseldatenträgern.

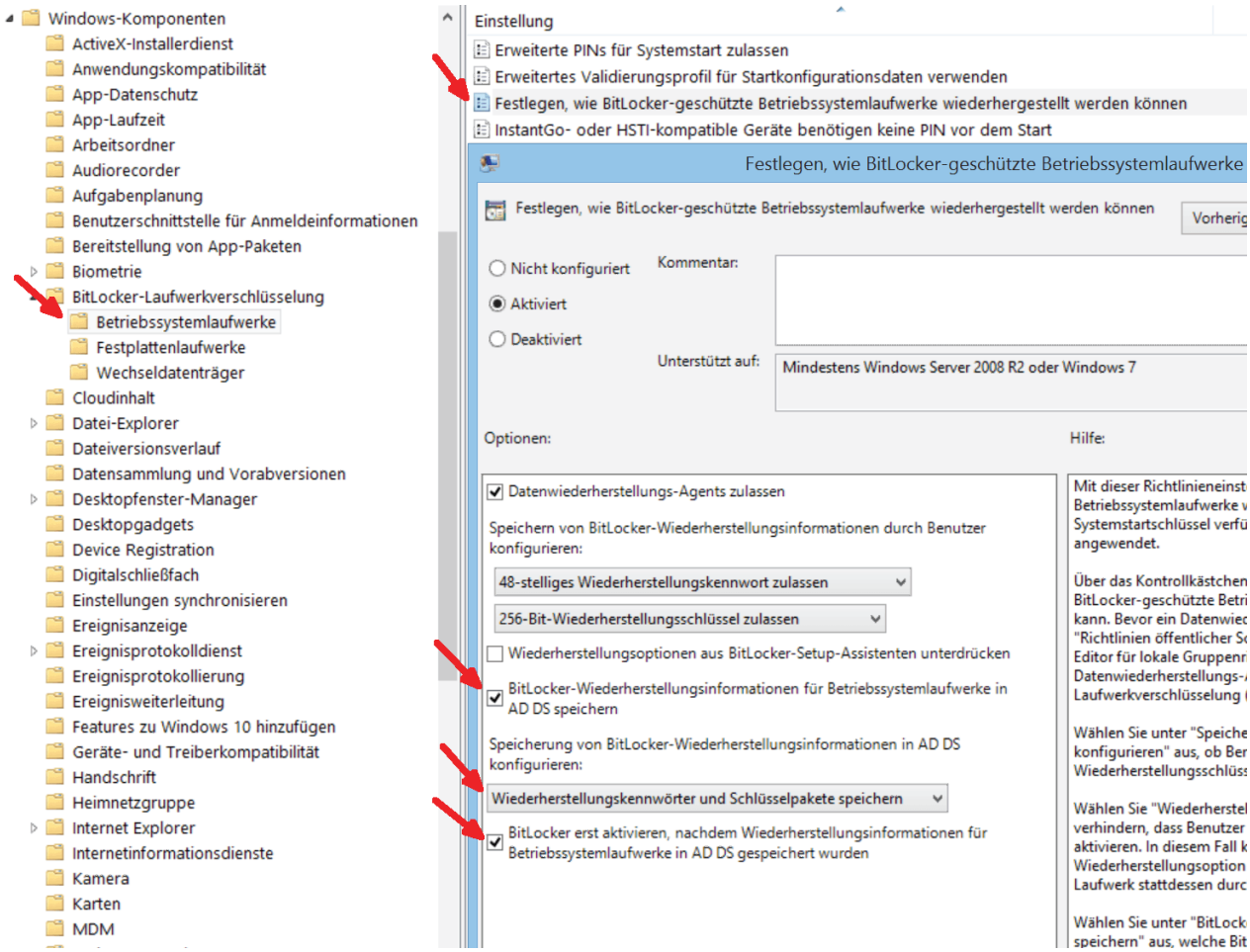
Für jeden Typ findet sich im GPO-Editor ein eigener Ordner mit den dazugehörigen Einstellungen. Eine davon heißt: *Festlegen, wie BitLocker geschützte <Laufwerkstyp> wiederhergestellt werden können.*



Die verschiedenen Laufwerkstypen lassen sich über eigene Einstellungen getrennt für BitLocker konfigurieren

Speicheroption für jeden Laufwerkstyp

Möchte man den Recovery Key für Betriebssystemlaufwerke im Active Directory speichern, dann aktiviert man diese Einstellung im betreffenden Ordner. Dort stellt man sicher, dass die Checkbox *BitLocker-Wiederherstellungsinformationen für Betriebssystemlaufwerke in AD DS speichern* angehakt ist.



GPO-Einstellung zur Sicherung von Recovery Keys für Systemlaufwerke im Active Directory

Darüber hinaus kann man hier konfigurieren, welche Daten im AD abgelegt werden. Zur Auswahl stehen *Wiederherstellungskennwort und Schlüsselpaket sichern* sowie *Nur Wiederherstellungskennwörter sichern*. Das Schlüsselpaket dient dem Wiederherstellen von Daten auf einem physikalisch beschädigten Laufwerk.

Zusätzlich ist es sinnvoll, die Option *BitLocker erst aktivieren, nachdem Wiederherstellungsinformationen für Betriebssystemlaufwerke in AD DS gespeichert wurden* anzuhaken. Das gewährleistet, dass BitLocker wartet, bis beispielsweise mobile Anwender wieder mit dem AD verbunden sind, bevor es die Daten chiffriert.

Schlüssel nachträglich manuell sichern

Sind Laufwerke bereits verschlüsselt, bevor man diese Gruppenrichtlinie aktiviert, dann greift diese nicht mehr und man muss den Key manuell in das Active Directory übertragen. Zuständig dafür ist das Kommandozeilen-Tool *manage-bde.exe*. Damit findet man zuerst die ID des numerischen Passworts für das Laufwerk c:

manage-bde -protectors -get c:

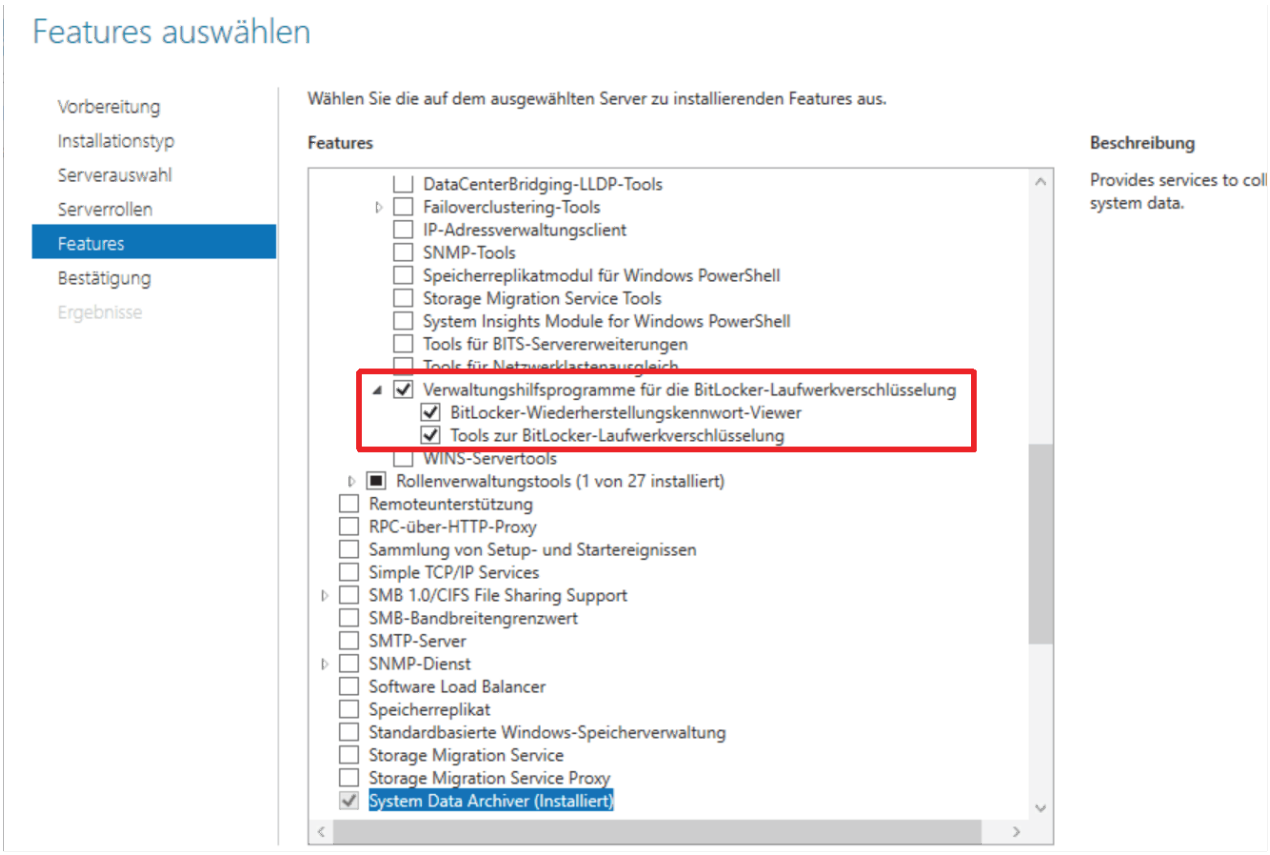
und übergibt diese in einem zweiten Aufruf an

manage-bde -protectors -adbackup c: -id {ID-des-numerischen-Passworts}

Wiederherstellungsschlüssel aus dem Active Directory auslesen

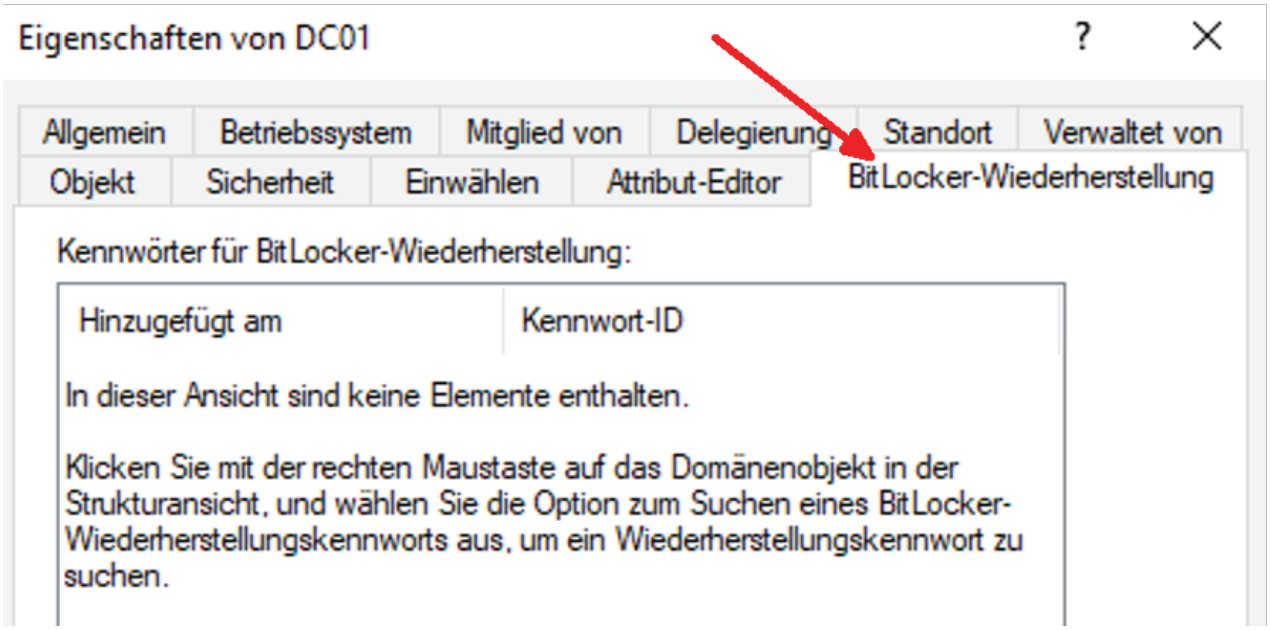
Um den Wiederherstellungsschlüssel auslesen zu können, ist es notwendig, zwei Features auf dem Server zu installieren, auf dem die Administratoren später an den Wiederherstellungsschlüssel gelangen möchten. Es handelt sich dabei um *BitLocker Wiederherstellungskennwort - Viewer* und *Tools zur BitLocker-Laufwerksverschlüsselung*.

Dies lässt sich über den Assistenten zum Hinzufügen von Rollen und Features im Server Manager erledigen, auf einer Workstation sind sie Bestandteil der RSAT.



BitLocker-Tools als Feature über den Server Manager hinzufügen

Danach sollte in *Active Directory-Benutzer und -Computer* beim Öffnen eines Computer-Objektes ein neuer Reiter mit der Beschriftung *BitLocker-Wiederherstellung* zu sehen sein.



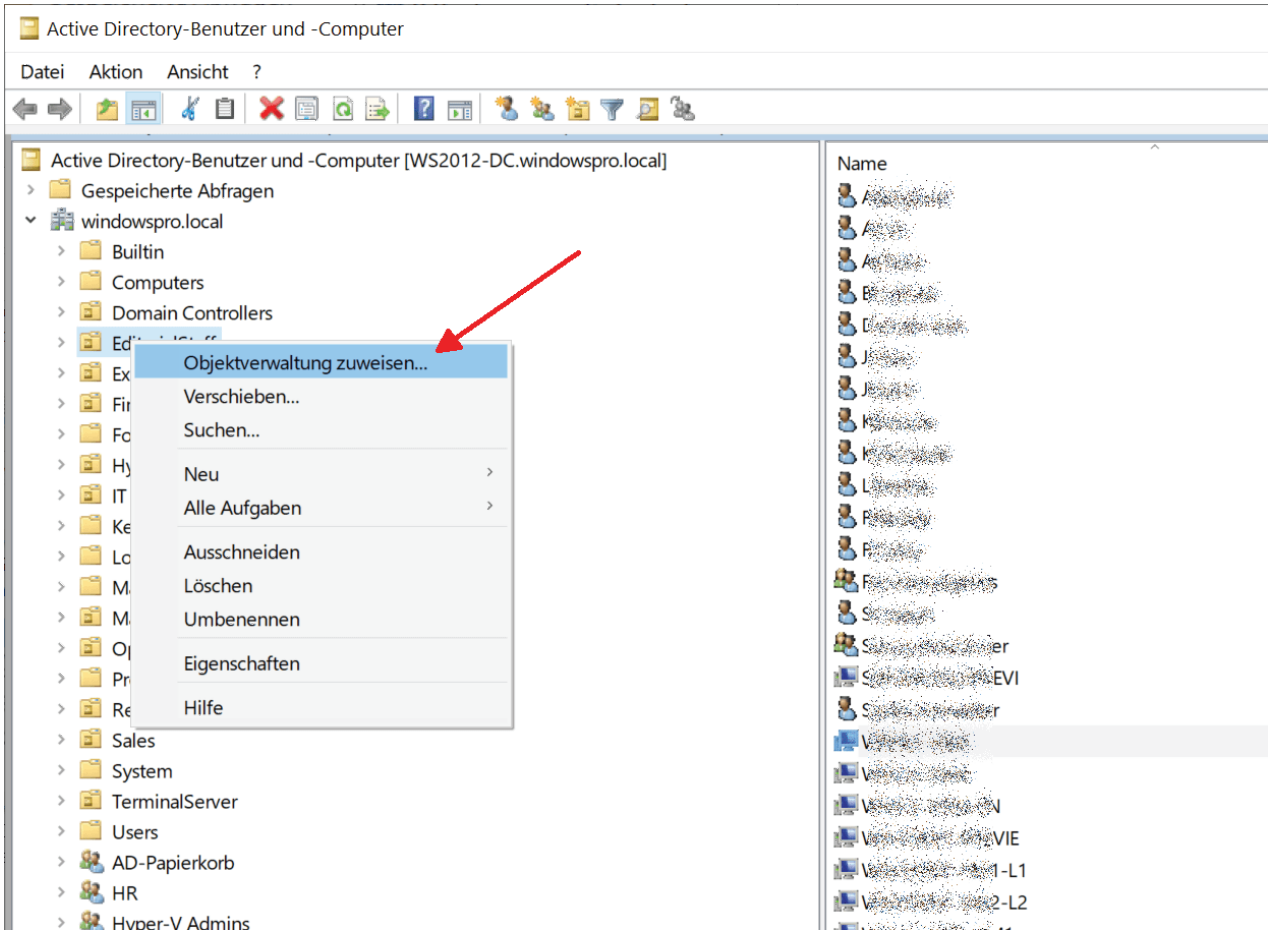
Durch die Installation der BitLocker-Tools erhält Active Directory-Benutzer und Computer eine Registerkarte für den Recovery Key

Bei Computern mit verschlüsselten Laufwerken würde nun hier der entsprechende Wiederherstellungsschlüssel stehen.

Delegierung

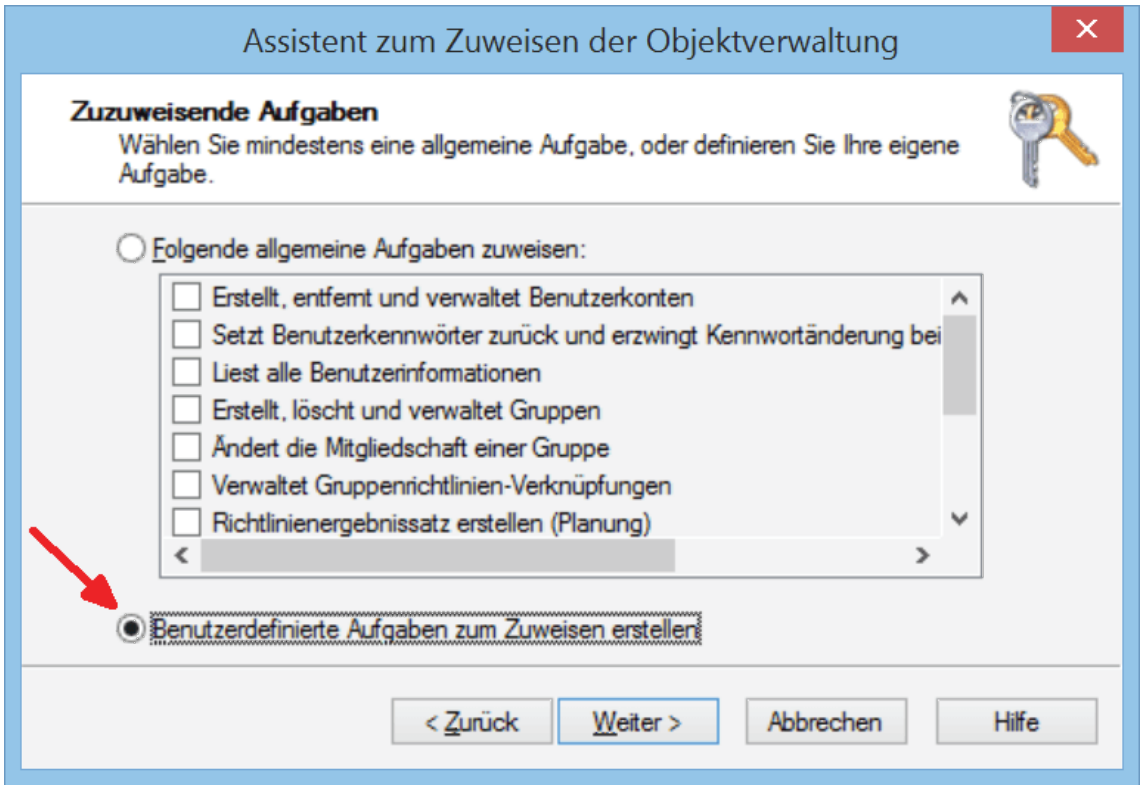
Standardmäßig können nur User der Gruppe der Domänen-Admins die BitLocker-Wiederherstellungsschlüssel anzeigen. Das reicht nicht aus, wenn zum Beispiel der Helpdesk in der Lage sein soll, auf die Recovery Keys zuzugreifen.

Um Benutzern diese Berechtigung einzuräumen, erstellt man eine Sicherheitsgruppe im Active Directory (als Name zum Beispiel *BitLocker*) und fügt ihr die gewünschten User hinzu. Danach führt man den Befehl *Objektverwaltung zuweisen* aus dem Kontextmenü der Organisationseinheit aus, in der sich die Computer befinden, deren Schlüssel die Gruppe anzeigen soll.



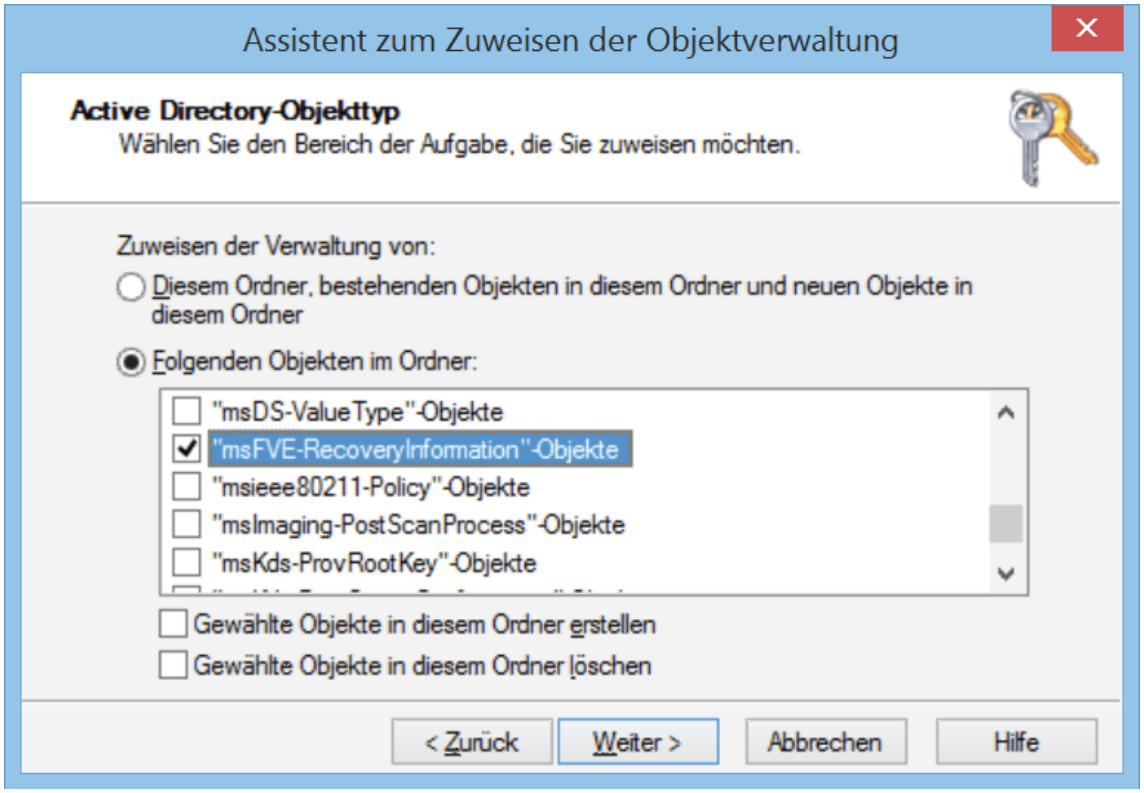
Den Befehl Objektverwaltung zuweisen aus dem Kontextmenü der OU ausführen

Im folgenden Dialog aktiviert man *Benutzerdefinierte Aufgaben zum Zuweisen erstellen*



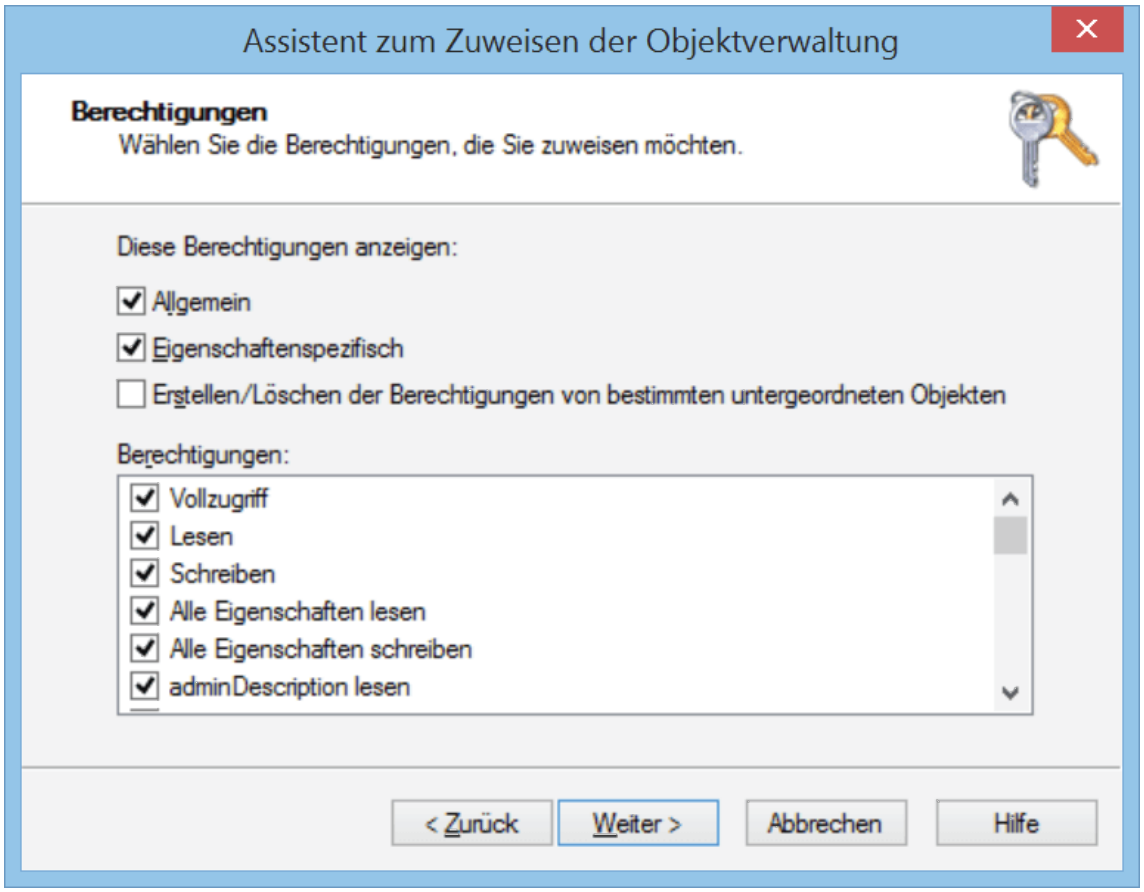
Auswahl von Benutzerdefinierte Aufgaben zum Zuweisen erstellen

Nun setzt man die Berechtigung für "msFVE-RecoveryInformation"-Objekte.



Berechtigung für msFVE-RecoveryInformation-Objekte vergeben

Erforderlich ist hier *Vollzugriff*.



Vollzugriff auf msFVE-RecoveryInformation-Objekte gewähren

Damit sind die User, welche sich in der Sicherheitsgruppe befinden in der Lage, den Wiederherstellungsschlüssel anzuzeigen.

BitLocker aktivieren

Mit Hilfe der Gruppenrichtlinien kann man für BitLocker zwar verschiedene Einstellungen vorgeben, aber die Verschlüsselung startet man damit nicht. Ebenso wenig erstellt man damit Protectors, ohne die BitLocker nicht aktiviert werden kann. Für diese Aufgabe bieten sich manage-bde, PowerShell oder Funktionen der WMI-Klasse Win32_EncryptableVolume an.

Grundsätzlich würden sich Admins einen Mechanismus wünschen, mit dem sie die BitLocker-Verschlüsselung zentral anstoßen könnten. Einen solchen bekommt man über verschiedene Lösungen für das Endpoint Management, aber nicht mit den Bordmitteln.

Automatische BitLocker-Aktivierung

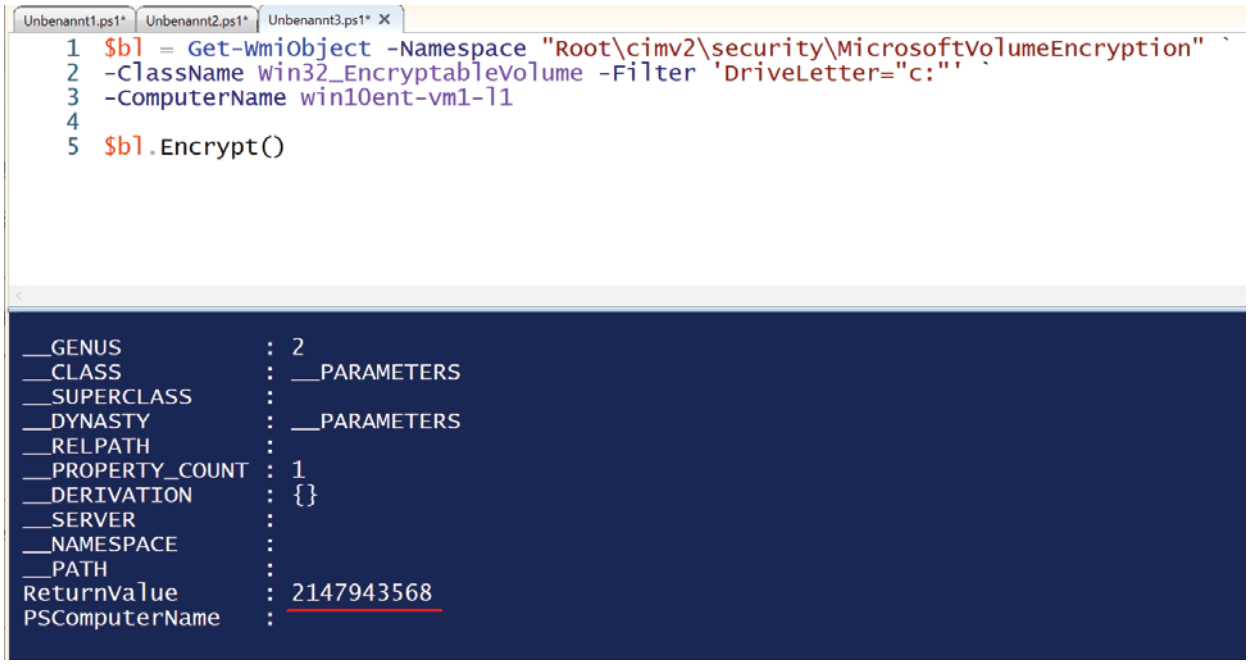
BitLocker kennt zwar eine automatische Verschlüsselung, aber diese greift nur unter ganz bestimmten Voraussetzungen. Dazu gehört eine moderne Hardware mit TPM (1.2 oder 2.0), auf der UEFI Secure Boot, Platform Secure Boot und DMA aktiviert sind.

Die Verschlüsselung startet aber erst dann, wenn sich der User an seinem Microsoft-Konto oder an Azure AD anmeldet. Arbeitet man jedoch mit lokalen oder Domänen-Accounts, dann funktioniert die automatische Verschlüsselung nicht.

In on-prem-Umgebungen muss man BitLocker daher auf andere Weise in Gang setzen. Dies kann man über das Dienstprogramm manage-bde oder ein PowerShell-Script mit den nativen BitLocker-Cmdlets oder WMI tun.

Protectors als Voraussetzung

Die Verschlüsselung kann nicht starten, bevor nicht zumindest ein Protector konfiguriert wurde. Versucht man es trotzdem, etwa über die WMI-Funktion encrypt(), dann erhält man den Fehler 0x8031002E (2150694958).



Die Methode encrypt() gibt den Fehlercode 2150694958 zurück, wenn kein Protector existiert

Sowohl manage-bde als auch *Enable-BitLocker* bieten die Möglichkeit, beim Aktivieren der Verschlüsselung auch gleich die Protectors einzurichten. Bei WMI sind dies getrennte Prozesse.

Eine solche Trennung zwischen dem Anlegen von Protectors und dem Aktivieren der Verschlüsselung ist unvermeidlich, wenn man die Protectors bereits während des OS-Deployment erzeugen möchte. Die Hürden dafür sind indes sehr hoch, weil BitLocker keine Möglichkeit bietet, Benutzer nachträglich zu zwingen, eine beim Deployment vergebene Standard-PIN zu ändern.

Zulässige Protectors bereitstellen

Egal welche Methode man wählt, sie kann nur Protectors erzeugen, die nicht im Widerspruch zu den Gruppenrichtlinien stehen. Bestimmte Protectors scheitern aber beim Versuch ihrer Einrichtung, auch wenn man sie nicht über ein GPO ausgeschlossen hat, weil sie bereits über die Default-Einstellungen nicht zulässig sind. Das gilt besonders für den Schutz von Systemlaufwerken durch ein Passwort alleine. Für diesen Versuch kassiert man den Fehler 0x8031006A (2150695018).

Die Konfiguration von TPM und PIN verhält sich hingegen umgekehrt. Wenn man diesen Protector nicht ausdrücklich über eine Gruppenrichtlinie zulässt, dann scheitert der Vorgang mit dem Fehler 0x80310060 (2150695008). Für TPM alleine gilt das hingegen nicht.

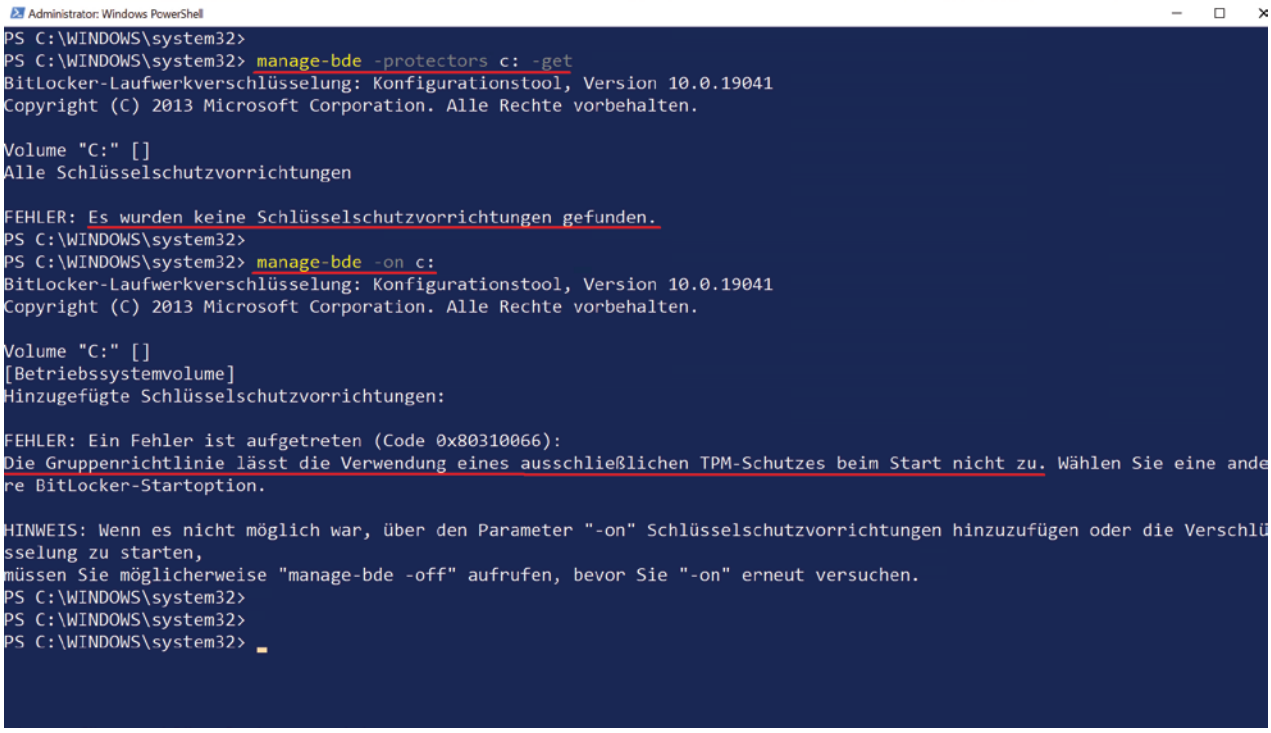
Schließlich gilt es noch zu bedenken, dass nicht alle Protectors für alle Laufwerke geeignet sind. TPM und Kombinationen mit TPM bleiben für Systemlaufwerke vorbehalten, während etwa Auto-Unlock nur bei Datenlaufwerken funktioniert.

Verschlüsselung aktivieren

Der dafür nötige Aufruf sieht mit manage-bde so aus:

```
manage-bde -on <Laufwerk:>
```

Wenn noch keine Protectors existieren, dann versucht dieser Aufruf, automatisch einen TPM-Protector einzurichten. Ist das etwa wegen einer Gruppenrichtlinie nicht möglich, dann scheitert der Befehl.



Gibt es noch keinen Protector, dann legt manage-bde per Voreinstellung einen TPM-Protector an. Dies kann an einer GPO-Einstellung scheitern

Alternativ kann man Protectors gleich an Ort und Stelle erzeugen, indem man dem Kommando die entsprechenden Parameter mitgibt:

- RecoveryPassword oder -rp
- RecoveryKey oder -rk
- StartupKey oder -sk
- Certificate oder -cert
- TPMAndPIN oder -tp
- TPMAndStartupKey oder -tsk
- TPMAndPINAndStartupKey oder -tpsk
- tpm
- Password oder -pw
- ADAccountOrGroup oder -sid

Ein Beispiel für das Systemlaufwerk könnte so aussehen:

manage-bde -on C: -RecoveryPassword -UsedSpaceOnly

Als zusätzliche Optionen stehen *UsedSpaceOnly* und *SkipHardwareTest* zur Verfügung, um nur den mit Daten belegten Plattenplatz zu verschlüsseln bzw. den Hardware-Test zu überspringen. Mit dem Parameter *ComputerName* bzw. *cn* kann man BitLocker auch remote auf anderen PCs aktivieren.

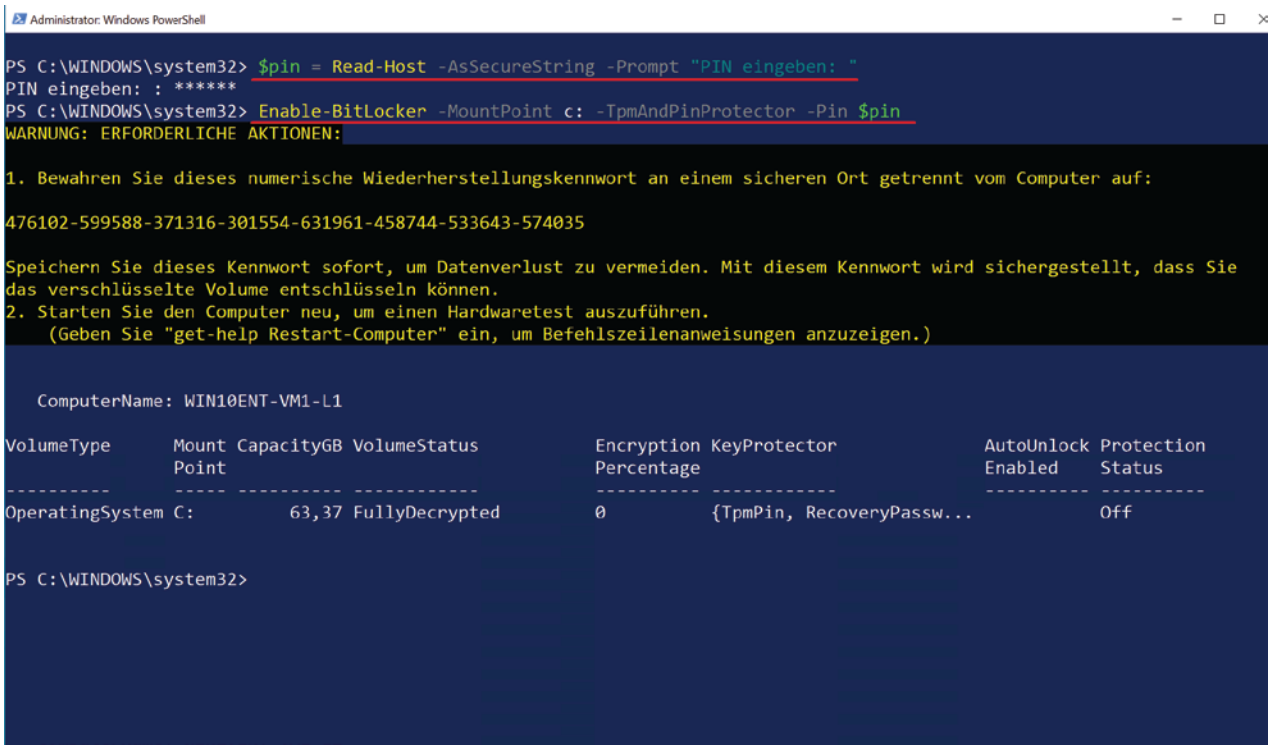
PowerShell

Bevorzugt man PowerShell, um BitLocker zu starten, dann ist das Cmdlet Enable-BitLocker dafür zuständig. Auch damit kann man gleich Protectors einrichten, die Parameter dafür sind gleich wie beim weiter oben beschriebenen *Add-BitLockerKeyProtector*.

```
$pin = Read-Host -AsSecureString -Prompt "PIN eingeben"

Enable-BitLocker -MountPoint c: -TpmAndPinProtector -Pin $pin
```

Auch hier kann man den Aufruf um die Schalter *SkipHardwareTest* und *UsedSpaceOnly* ergänzen.



BitLocker aktivieren und gleichzeitig einen TPMandPIN-Protector anlegen.

Der Recovery Key existiert in diesem Beispiel bereits

Für das Remote-Management fehlt der Parameter *ComputerName*, so dass man eine Session auf dem Ziel-PC öffnen und den Befehl dort ausführen müsste.

WMI

Die WMI-Klasse Win32_EncryptableVolume bietet für diesen Zweck die Funktionen *Encrypt()* und *EncryptAfterHardwareTest()*. Letztere erfordert einen Neustart des Rechners. Beide setzen voraus, dass die benötigten Protectors existieren, sie lassen sich mit diesen Methoden nicht erstellen.

Hier ein Beispielaufruf:

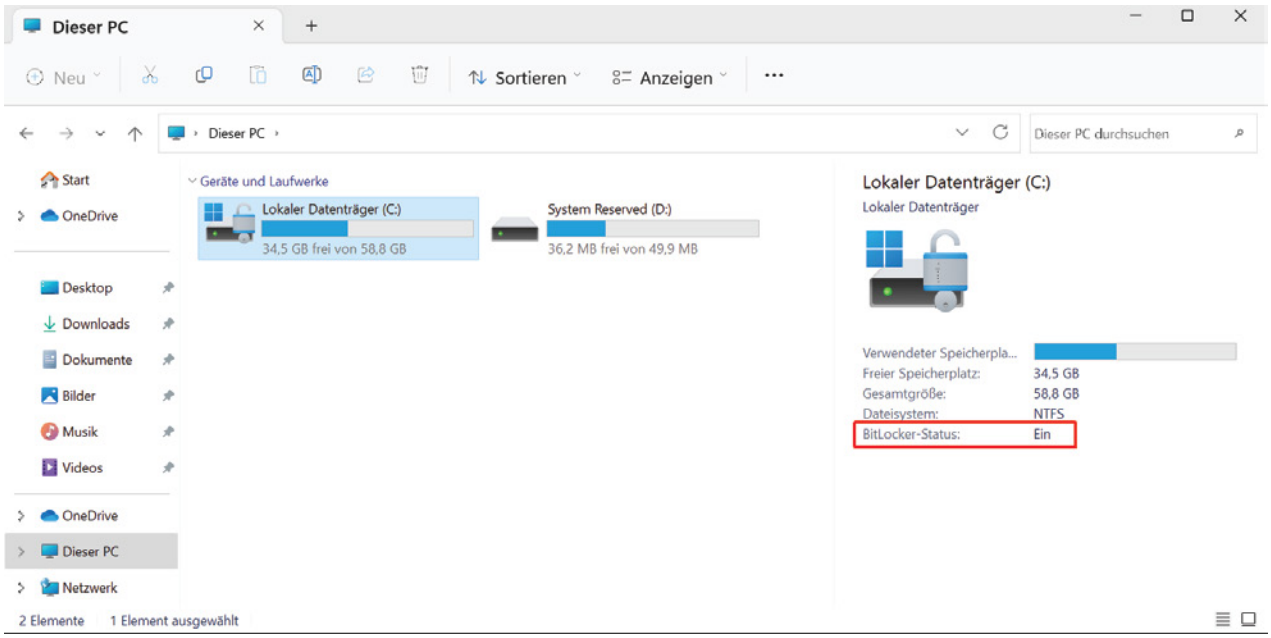
```
$bl = Get-WmiObject -ComputerName win11-vm1-l1`
-Namespace "Root\cimv2\security\MicrosoftVolumeEncryption" `
-ClassName Win32_EncryptableVolume -Filter 'DriveLetter="c:"'
$bl.Encrypt()
```

Wie man am Parameter *ComputerName* erkennt, aktiviert dieses Kommando die Verschlüsselung auf einem Remote-PC. Beide Funktionen sind nur über GetWmiObject, aber nicht mit *Get-CimInstance* verfügbar.

Verschlüsselung des Systemlaufwerks remote prüfen

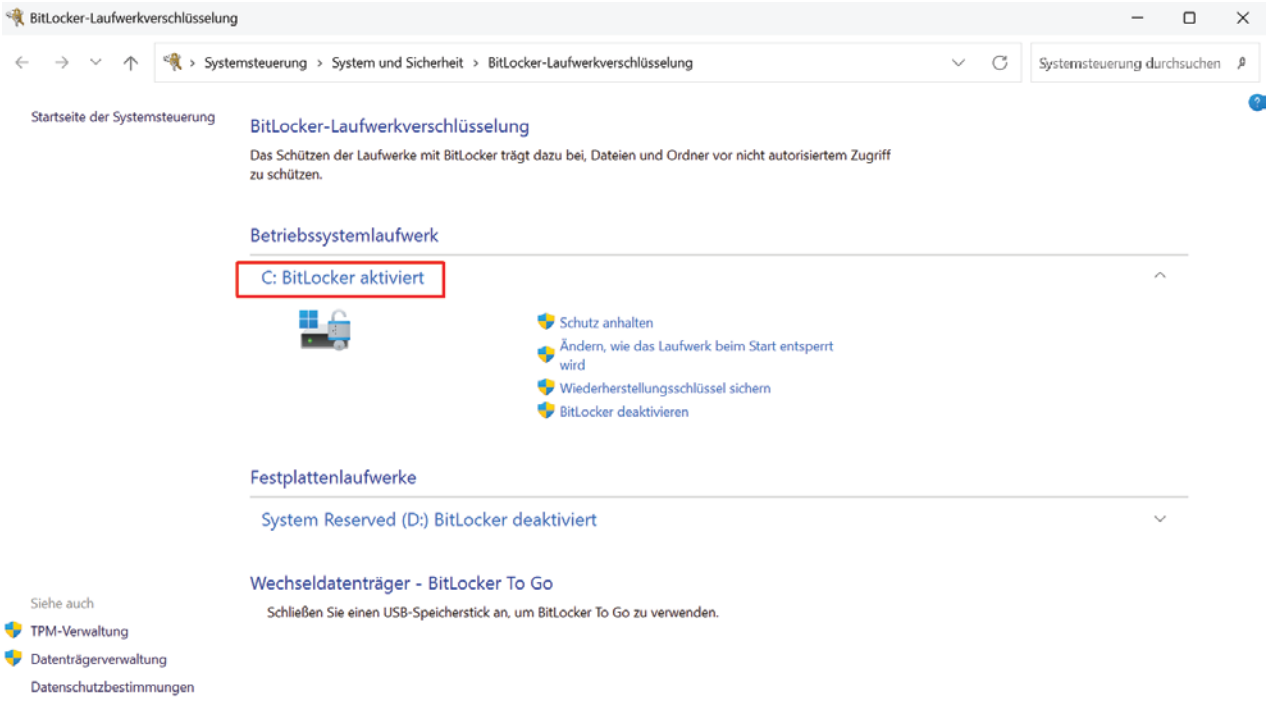
Wenn man BitLocker über die Bordmittel aktiviert, dann liefern diese keinen Report über den Verschlüsselungsstatus der ganzen Umgebung. Inaktiven BitLocker-Schutz kann man aber mit dem Dienstprogramm manage-bcd und PowerShell erkennen.

Möchte man herausfinden, ob das Systemlaufwerk des lokalen Rechners verschlüsselt ist, dann zeigt man im Explorer einfach die Eigenschaften von C: im Detailbereich an.



BitLocker-Status im Explorer einsehen

Alternativ bietet das BitLocker-Applet in der Systemsteuerung die gleiche Information an.



BitLocker-Status im Applet der Systemsteuerung prüfen

Die Angaben auf der GUI sind jedoch nicht nur rudimentär, sondern auch nicht praktikabel für eine Remote-Abfrage.

BitLocker-Status mit manage-bde ermitteln

Für diese Aufgabe eignet sich das Dienstprogramm *manage-bde:*

```
manage-bde -status -computername Win11PC c:
```

In diesem Beispiel erhält man die BitLocker-Informationen zum Laufwerk c: auf dem Computer *Win11PC*. Diese umfassen unter anderem Angaben zur Größe des Laufwerks, zur BitLocker-Version, den Konvertierungsstatus, die Verschlüsselungsmethode oder die konfigurierten Protectors.

Informationen zum Status von BitLocker von einem Remote-PC mit manage-bde abrufen

Wenn sich manage-bde nicht mit dem Host verbinden kann, dann sollte man prüfen, ob die Firewall-Regel für WMI (eingehend) auf dem Ziel-Rechner aktiviert ist:

```
Get-NetFirewallRule -Name *WMI* |
select DisplayName, Profile, Enabled
```

Ist das nicht der Fall, dann aktiviert man sie über Gruppenrichtlinien, PowerShell oder netsh.exe. In PowerShell erledigt man diese Aufgabe nach diesem Muster:

```
Set-NetFirewallRule -Name WMI-WINMGMT-In-TCP-NoScope `
-Enabled True -Profile Domain
```

BitLocker-Status mit PowerShell ermitteln

PowerShell bietet mit *Get-BitLockerVolume* ein Cmdlet, das ebenfalls den BitLocker-Status abfragen kann:

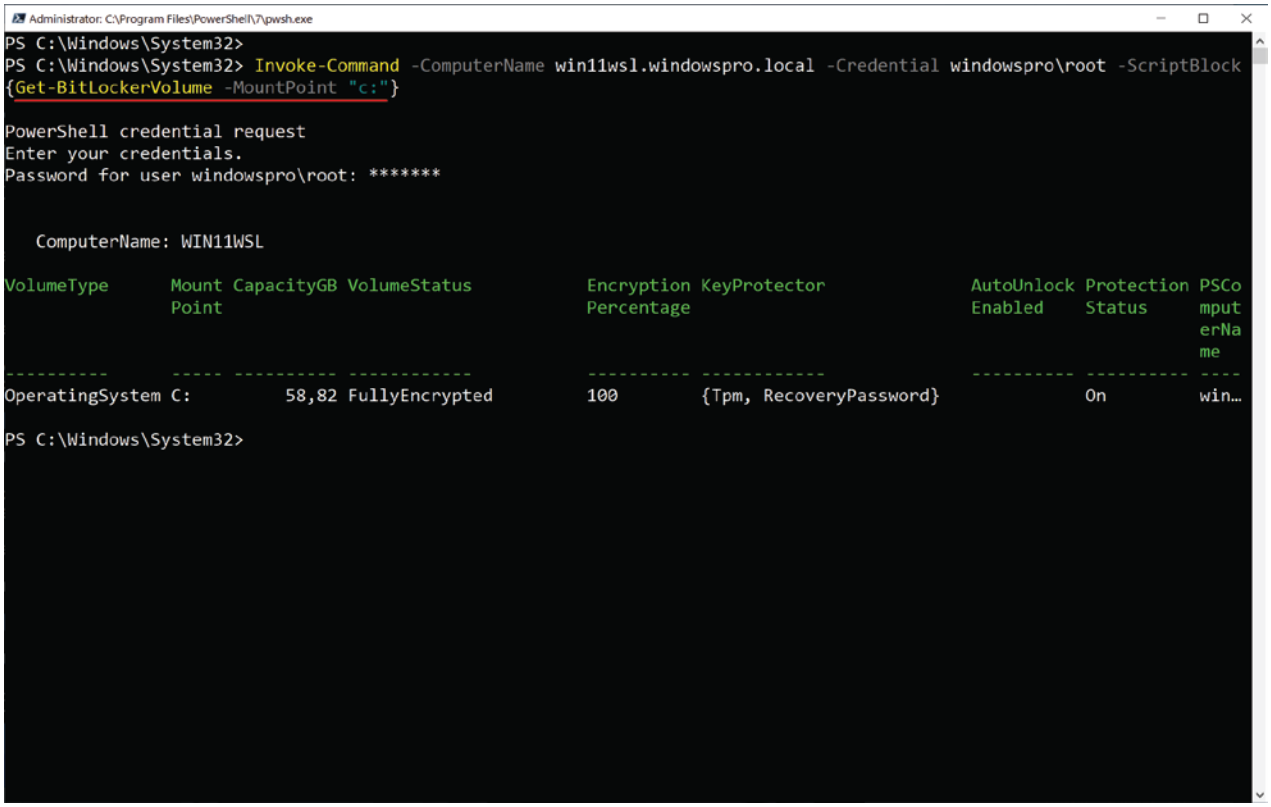
```
Get-BitLockerVolume -MountPoint "c:"
```

Mit diesem Aufruf erhält man Auskunft über das Laufwerk C: des lokalen Rechners.

Das Cmdlet unterstützt jedoch nicht den Parameter *ComputerName,* so dass man keinen entfernten PC untersuchen kann. Es bleibt jedoch die Möglichkeit, den Aufruf an *Invoke-Command* zu übergeben:

```
Invoke-Command -ComputerName win11PC `
-ScriptBlock {Get-BitLockerVolume -MountPoint "c:"}
```

Damit diese Abfrage klappt, muss WinRM auf allen Geräten konfiguriert sein und sie muss aus einer PowerShell-Session mit erhöhten Rechten erfolgen, bzw. man gibt den privilegierten User über den Parameter *Credential* an.



Status von BitLocker mit Hilfe von Get-BitLockerVolume remote abfragen

BitLocker-Status über WMI abfragen

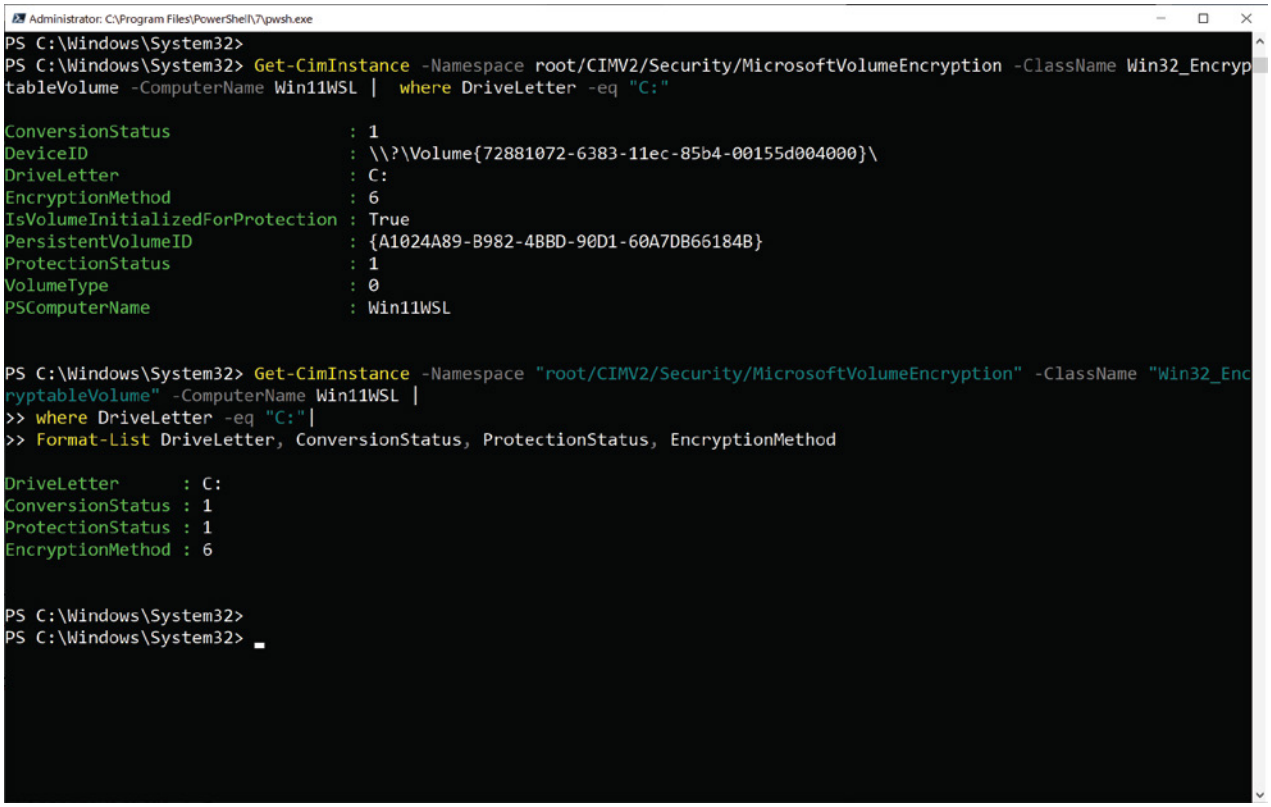
Alternativ zum obigen Cmdlet kann man eine WMI-Abfrage absetzen, um die BitLocker-Infos zu erhalten:

```
Get-WmiObject("Win32_EncryptableVolume") -ComputerName Win11WSL `
-Namespace "root\CIMV2\Security\MicrosoftVolumeEncryption" |
where DriveLetter -eq "C:" |
Format-List DriveLetter, ConversionStatus, ProtectionStatus, EncryptionMethod
```

Der Aufruf über das CIM-Gegenstück von *Get-WmiObject* sieht identisch aus:

```
Get-CimInstance -ComputerName Win11 -ClassName "Win32_EncryptableVolume" `
-Namespace "root/CIMV2/Security/MicrosoftVolumeEncryption"  |
where DriveLetter -eq "C:"|
Format-List DriveLetter, ConversionStatus, ProtectionStatus, EncryptionMethod
```

Der Nachteil dieses Verfahrens besteht darin, dass man für *ConversionStatus, ProtectionStatus und EncryptionMethod* numerische Werte erhält, die man dann mit Hilfe dieser Tabellen übersetzen muss.



Informationen zu BitLocker über WMI abrufen

Computer aus dem Active Directory untersuchen

Bei einer größeren Zahl von Computern ist es wahrscheinlich am günstigsten, manage-bde mit PowerShell zu kombinieren:

```
Get-ADComputer -Filter *' -SearchBase "OU=HR,DC=contoso,DC=com"| foreach{
  if(Test-Connection -ComputerName $_.DNSHostName -Quiet){
   manage-bde -status -cn $_.DNSHostName c: |
   where {$_ -match '(Computername|Schutzstatus|Konvertierungsstatus)'}
    }
}
```

Dieses Beispiel ruft die Namen aller Computer aus der OU namens HR ab, prüft mit Test-Connection, ob die Rechner erreichbar sind, und startet dann manage-bde, um den Status des Laufwerks c: zu ermitteln.

Status von BitLocker über ein PowerShell-Script mit manage-bde abfragen

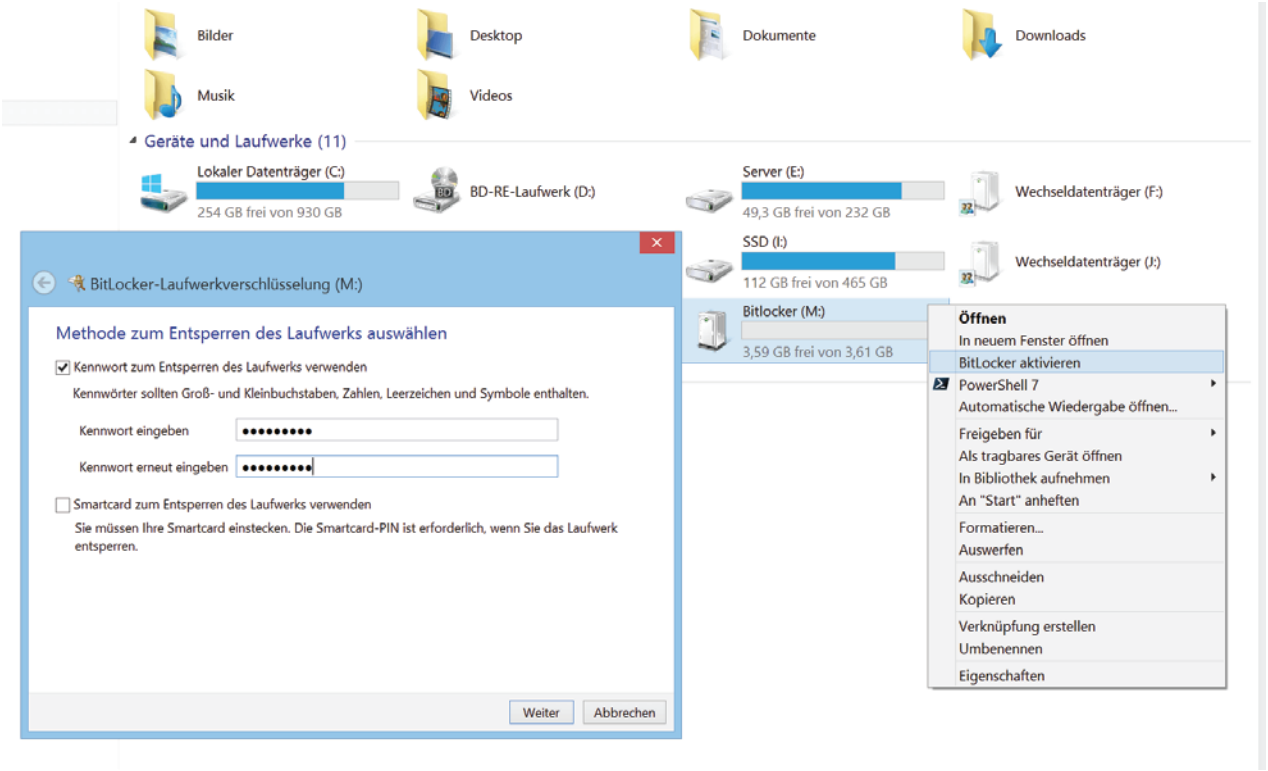
Über den regulären Ausdruck mit dem match-Operator filtert man die relevanten Ausgaben. Auf einem englischen Windows müsste man dafür '(Computer Name|Protection Status|Conversion Status)' verwenden.

USB-Laufwerken mit BitLocker To Go verschlüsseln

Wenn Unternehmen den unkontrollierten Abfluss von Daten verhindern wollen, dann gilt ihre besondere Aufmerksamkeit den Wechseldatenträgern. In vielen Firmen ist es gängige Praxis, USB-Geräte pauschal zu blockieren oder zumindest Device-Typen zu bannen.

Wenn eine solche strikte Politik nicht umsetzbar ist, etwa weil externe Laufwerke für den Datenaustausch benötigt werden, dann kann man zumindest dafür sorgen, dass die darauf befindlichen Daten für Unbefugte nicht lesbar sind. Diese Aufgabe übernimmt seit Windows 7 die Funktion BitLocker To Go.

Standardmäßig können Benutzer der Editionen Pro und Enterprise USB-Datenträger nach eigenem Gutdünken verschlüsseln, indem sie den entsprechenden Befehl aus dem Kontextmenü des Laufwerks ausführen oder den Vorgang in der Systemsteuerung unter *System und Sicherheit => BitLocker-Laufwerkverschlüsselung* starten.

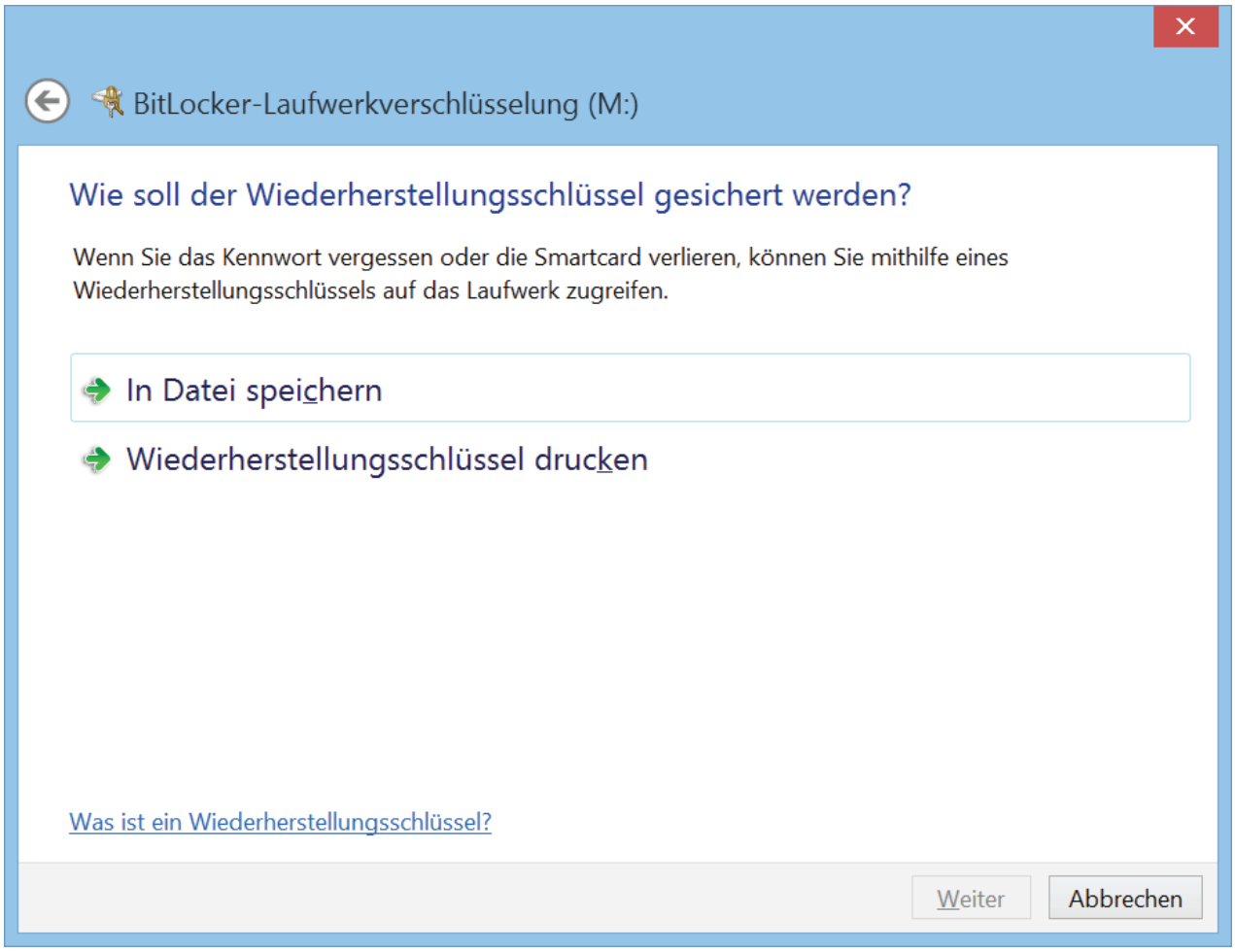


Benutzer können USB-Laufwerke in Eigenregie mit BitLocker verschlüsseln

Zentrale Konfiguration wichtiger Parameter

In verwalteten Umgebungen wird man es aber nicht den Endanwendern überlassen, ob sie Datenträger verschlüsseln.

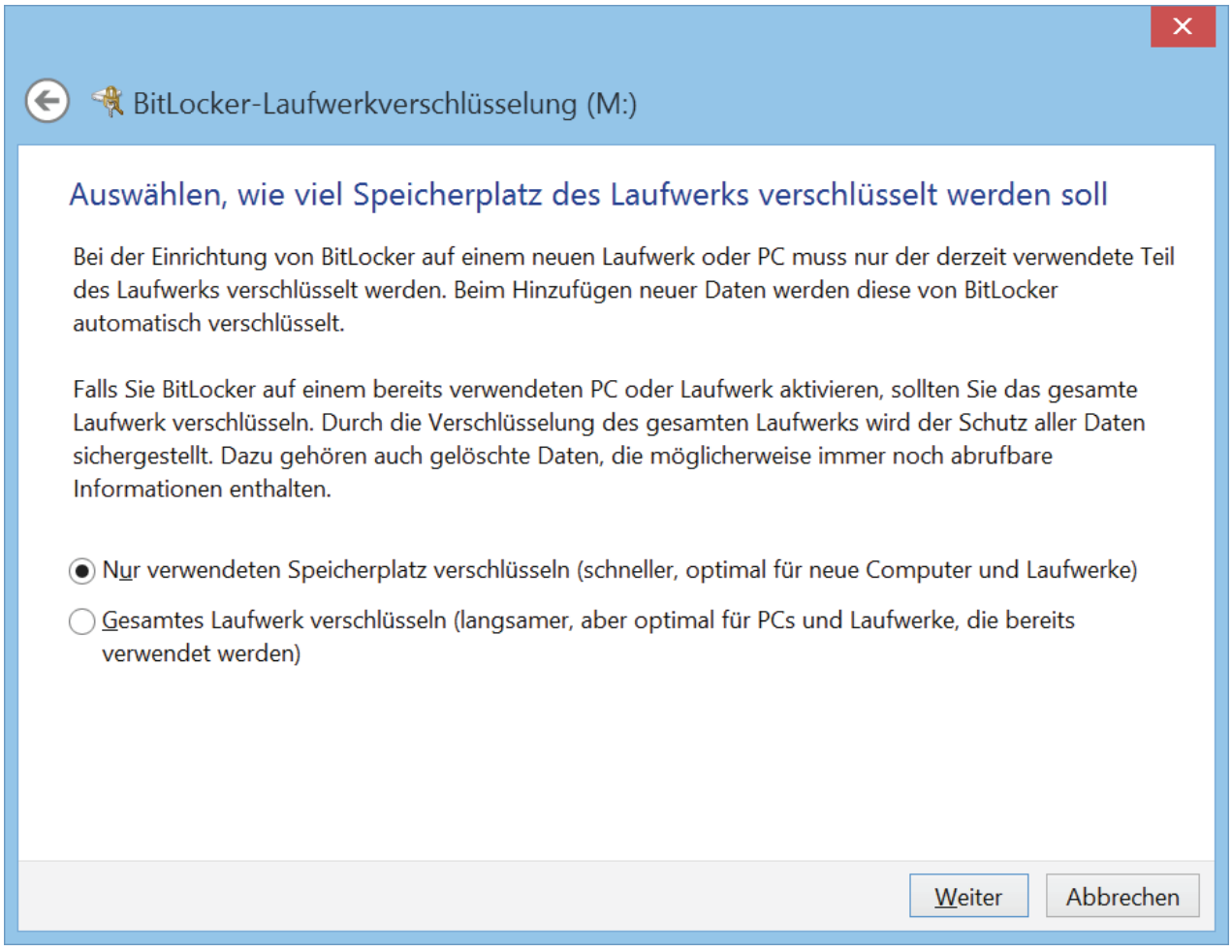
Hinzu kommt, dass sie dabei Entscheidungen treffen müssen, die einen reibungslosen und effizienten Einsatz des Features beeinträchtigen. Das gilt etwa für die Art, wie Wiederherstellungsschlüssel gesichert werden sollen, oder die Methode (voll oder verwendeten Speicherplatz).



Standardmäßig müssen sich die Benutzer selbst um die Aufbewahrung des Keys kümmern

Eine solche Auswahl kann der Administrator zentral über Gruppenrichtlinien treffen und dafür sorgen, dass etwa die Recovery Keys nicht verloren gehen oder unsachgemäß aufbewahrt werden.

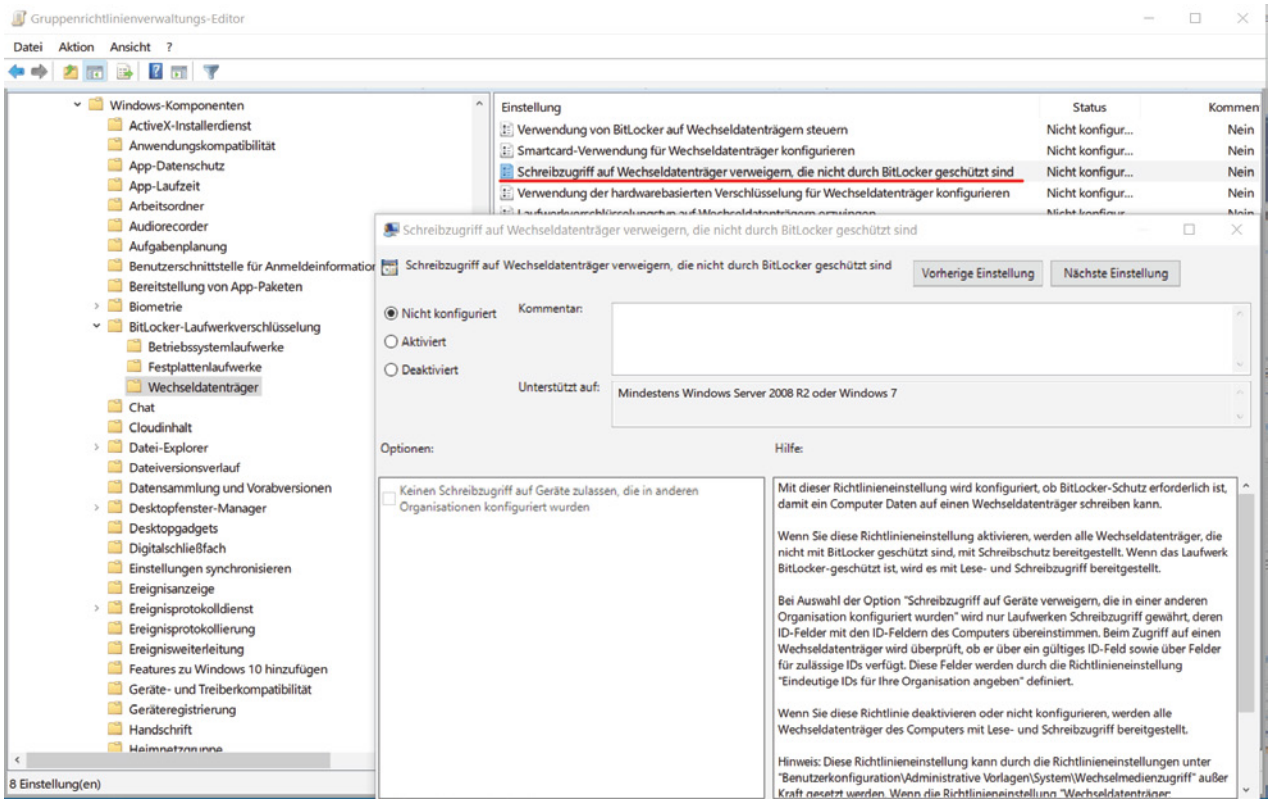
Ähnliches gilt für die Alternative zwischen der Verschlüsselung des ganzen oder nur des benutzten Speicherbereichs. Letztere spart zwar Zeit, aber zuvor vorhandene und mittlerweile gelöschte Daten wären aber ungeschützt.



Ohne Anpassung über Gruppenrichtlinien entscheidet der User über die Verschlüsselungsmethode

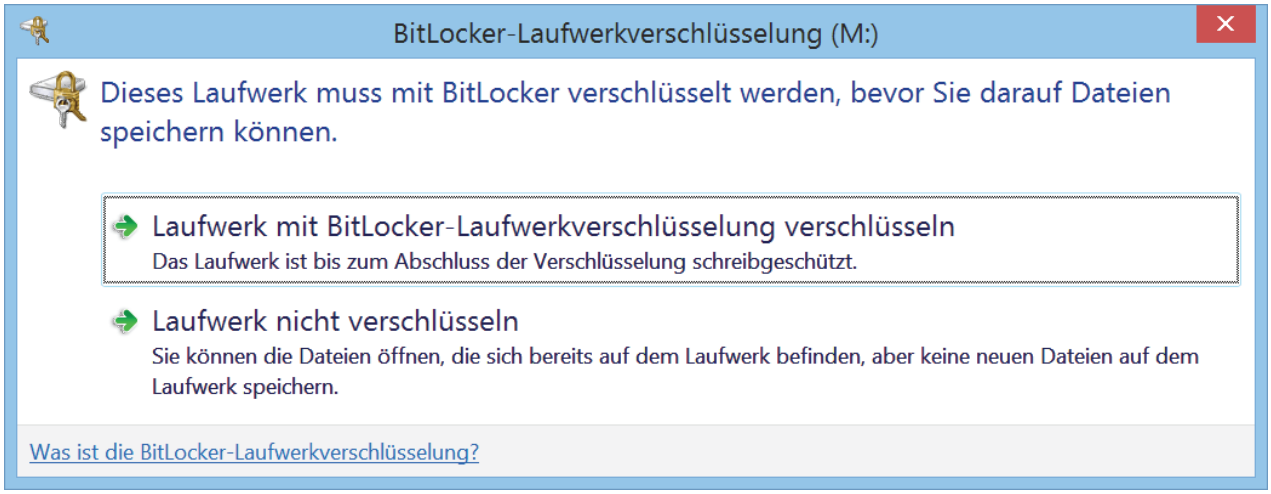
Die Einstellungen für BitLocker To Go finden sich unter *Computerkonfiguration => Richtlinien => Administrative Vorlagen => Windows-Komponenten => BitLocker-Laufwerksverschlüsselung => Wechseldatenträger.*

Um die Verschlüsselung von externen Laufwerken zu erzwingen, aktiviert man dort *Schreibzugriff auf Wechseldatenträger verweigern, die nicht durch BitLocker geschützt sind.*



Diese Option verhindert, dass Anwender Daten auf unverschlüsselte Wechseldatenträger speichern

Diese Einstellung bewirkt jedoch nicht, dass BitLocker etwa auf USB-Sticks automatisch im Hintergrund eingeschaltet wird, sobald der Benutzer das Gerät an den Rechner ansteckt. Vielmehr erhält er den Hinweis, dass Daten nur gespeichert werden können, nachdem BitLocker aktiviert wurde.

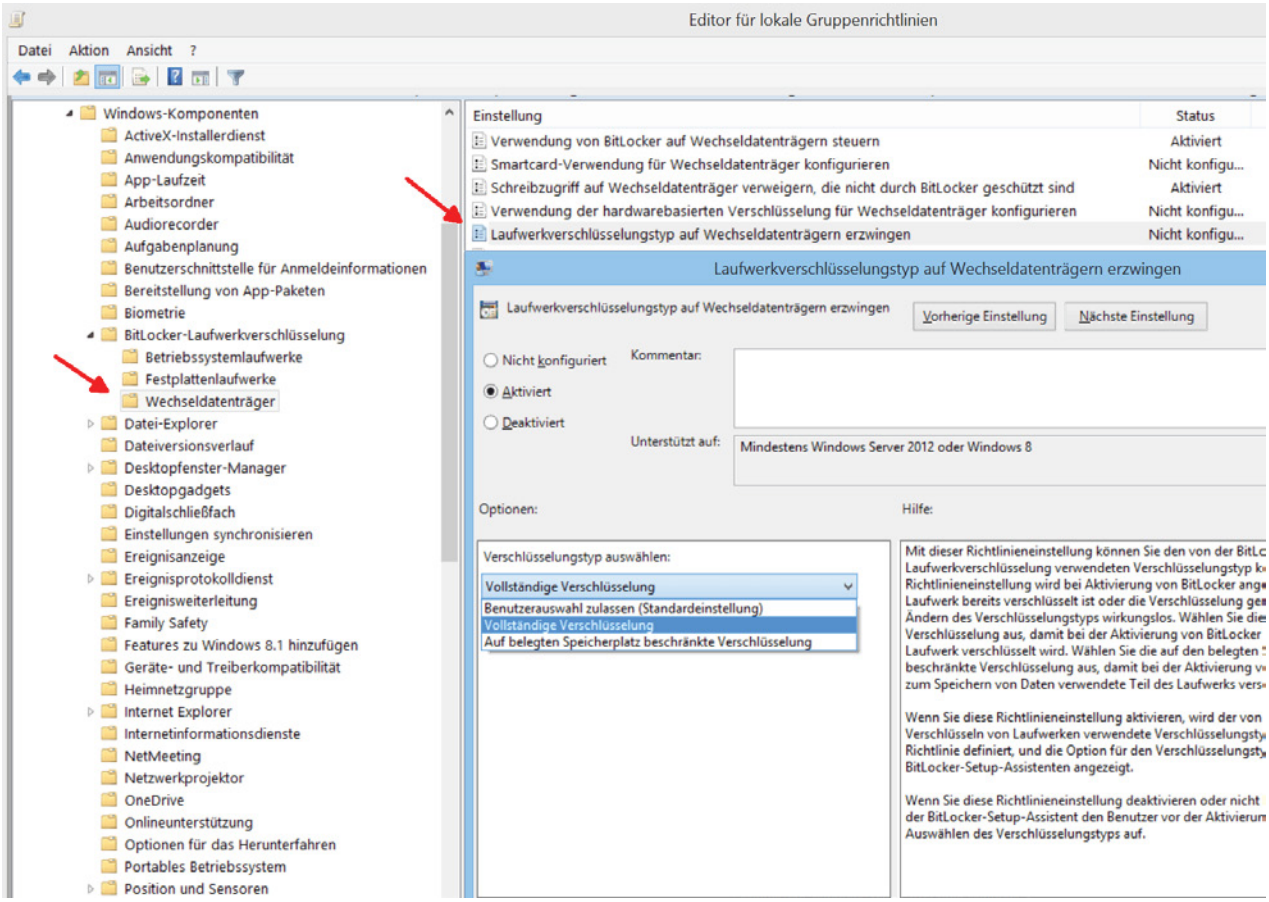


Benutzer können aus dem Hinweis den Assistenten für BitLocker To Go starten

Der Dialog bietet an, das Laufwerk zu verschlüsseln. Diese Option startet den gleichen Assistenten wie der oben erwähnte Befehl aus dem Kontextmenü des Datenträgers. Durch weitere Gruppenrichtlinien kann man dort aber einige Schritte überspringen.

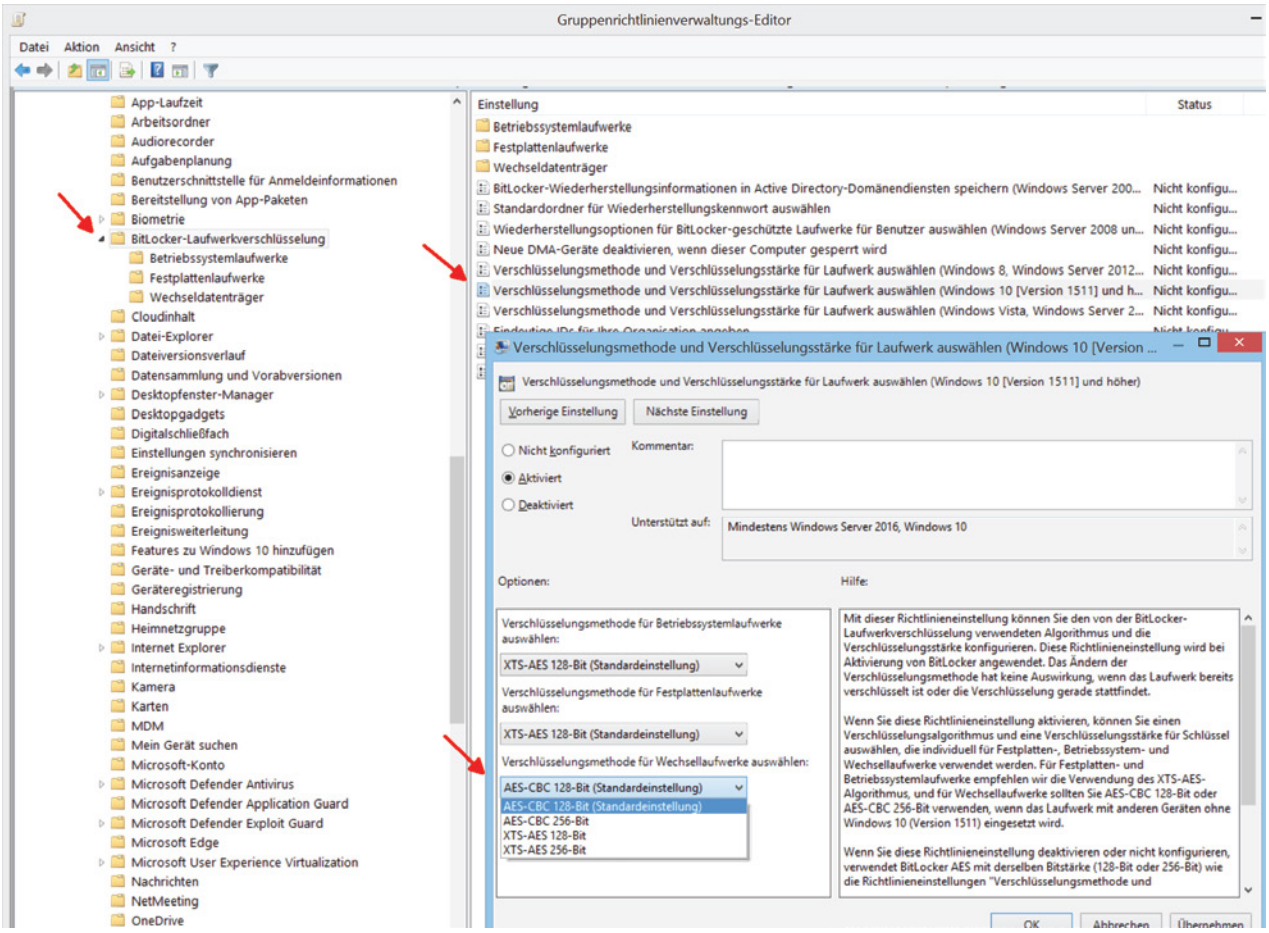
Dialoge aus Assistenten ausblenden

Dazu gehört die Einstellung *Laufwerkverschlüsselungstyp auf Wechseldatenträgern erzwingen*. Mit ihr legt man fest, ob der gesamte oder nur der benutzte Speicherbereich kodiert werden soll.



Art der Verschlüsselung via GPO vorgeben

Zusätzlich kann man bei den globalen BitLocker-Einstellungen den Algorithmus festlegen, und zwar mit *Verschlüsselungsmethode und Verschlüsselungsstärke für Laufwerk auswählen (Windows 10 [Version 1511] und höher)*.

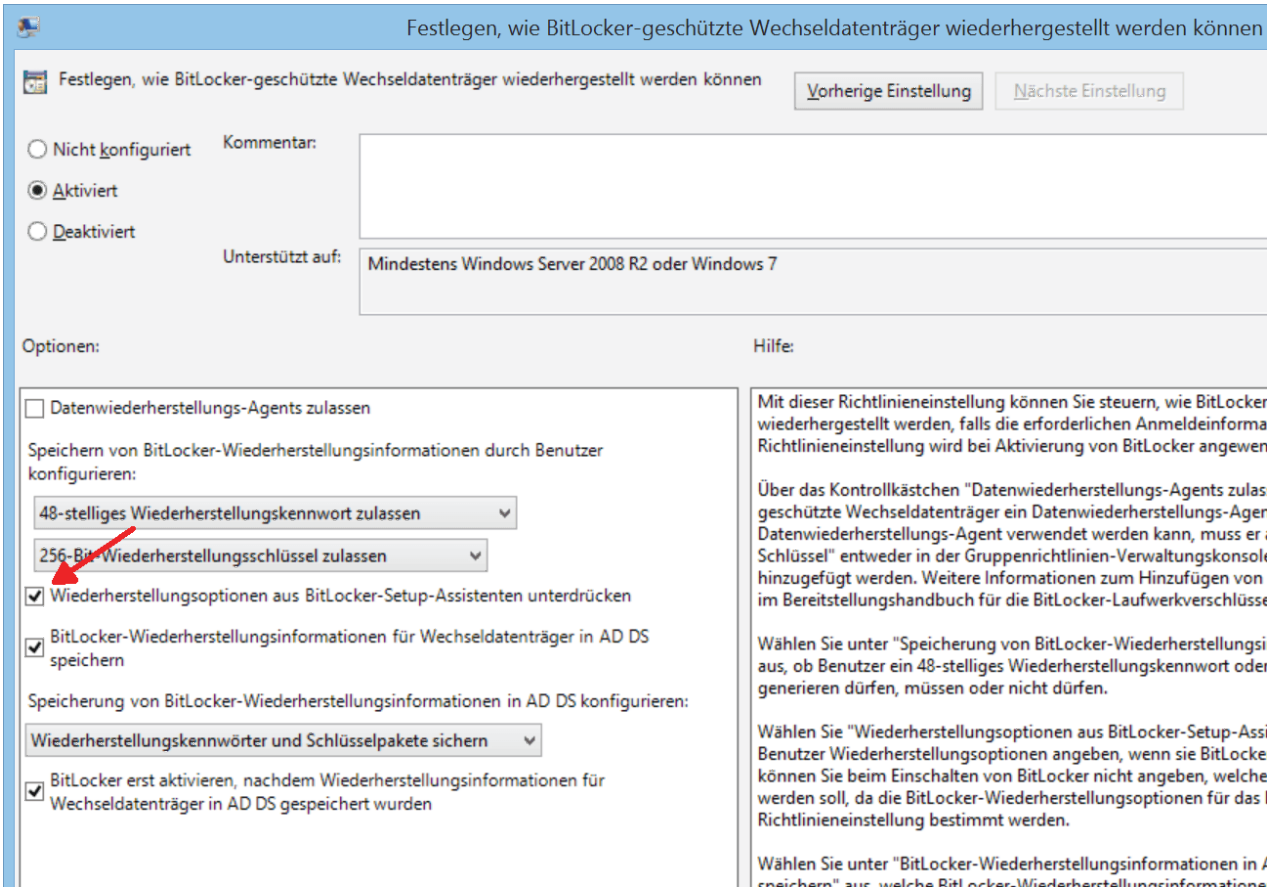


Algorithmus für die Verschlüsselung per GPO festlegen

Ein ganz wesentlicher Punkt betrifft die Frage, wie und wo die Wiederherstellungsschlüssel gesichert werden sollen. Ohne Vorgabe über die Gruppenrichtlinien kann der User zwischen dem Speichern in einer Datei und dem Ausdrucken wählen. Belässt man es dabei, dann muss man mit Anfragen an den Helpdesk wegen verlorener Keys oder mit Sicherheitslücken rechnen.

Wiederherstellungsschlüssel im AD speichern

In verwalteten Umgebung wird man die Wiederherstellungsschlüssel bevorzugt im Active Directory hinterlegen. Zuständig ist dafür die Einstellung *Festlegen, wie BitLocker-geschützte Wechseldatenträger wiederhergestellt werden können*. Das Vorgehen erfolgt nach dem gleichen Muster wie oben beschrieben für Systemlaufwerke.



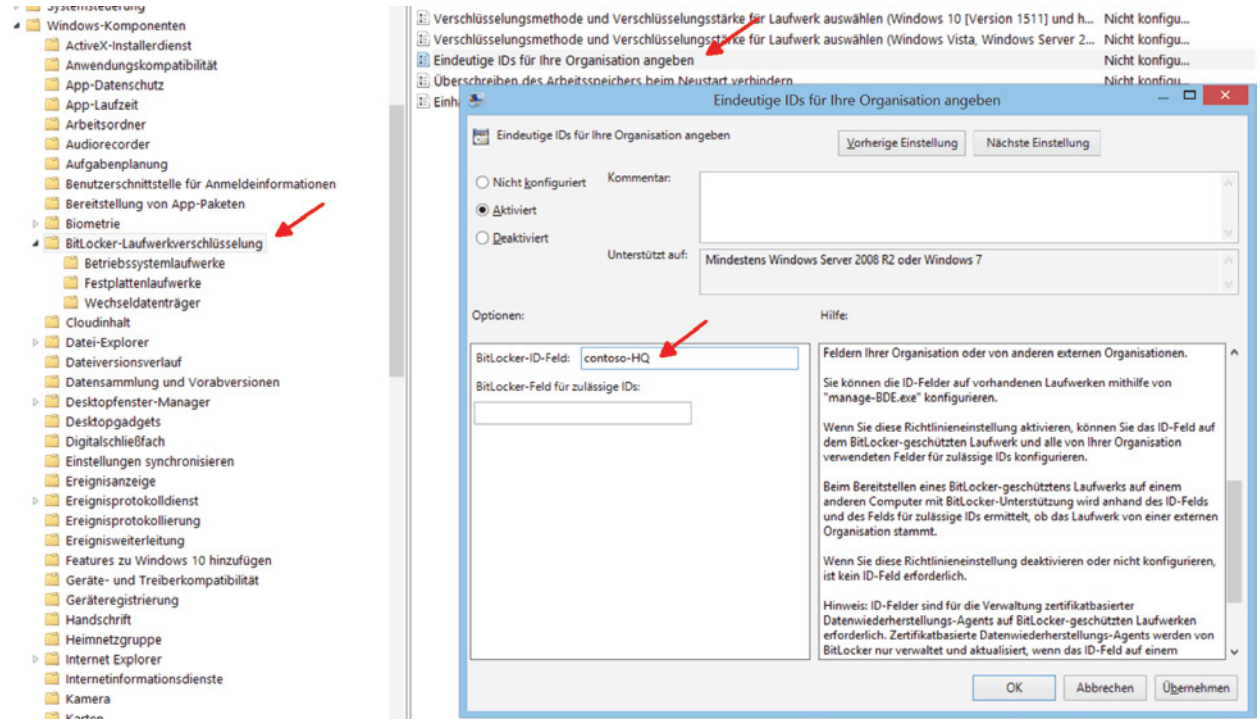
Über diese Option kann man den Dialog zum Speichern der Recovery Keys ausblenden

Wenn man dort die Option *Wiederherstellungsoptionen aus BitLocker-Setup-Assistent unterdrücken* aktiviert, dann wird der oben erwähnte Dialog für die Sicherung des Keys übersprungen. Die Benutzer können den Wiederherstellungsschlüssel somit nicht selbst speichern.

Datenträger mit ID markieren

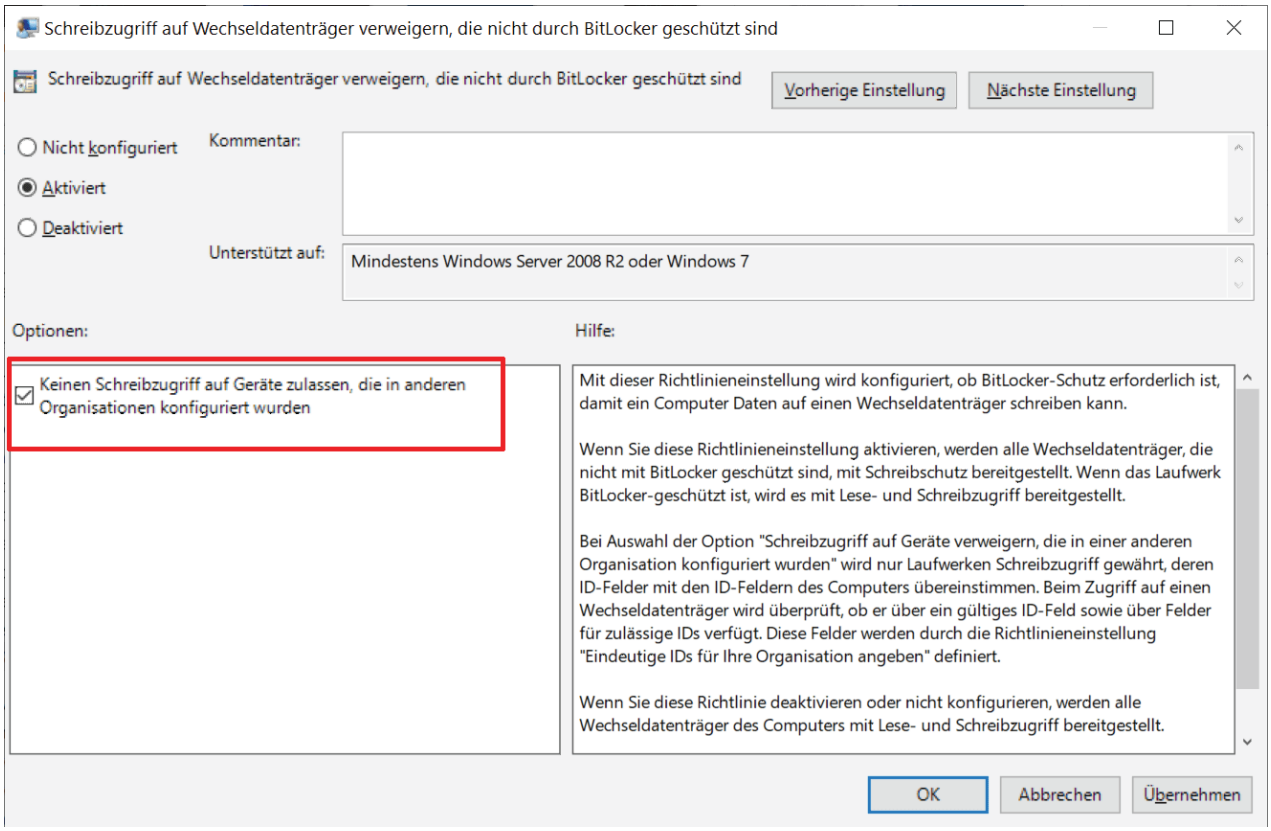
Das Problem verlorener Recovery Keys kann aber trotzdem auftreten, wenn ein Benutzer bereits früher einen USB-Stick mit BitLocker verschlüsselt hat. Um auszuschließen, dass er auf diesen auch nach der Konfiguration des GPO weiterhin Daten speichert, kann man die Laufwerke mit einer Organisations-ID versehen.

Zuständig dafür ist die Einstellung *Eindeutige IDs für Ihre Organisation angeben* im Zusammenspiel mit *Schreibzugriff auf Wechseldatenträger verweigern, die nicht durch BitLocker geschützt sind.* Sie versieht jedes Wechsellaufwerk mit der betreffenden Kennung. Dabei darf es sich um einen beliebigen Wert mit bis zu 260 Zeichen handeln.



Über die Organisations-ID kann man die zulässigen Geräte weiter einschränken

Zusätzlich benötigt man dafür die Option *Keinen Schreibzugriff auf Geräte zulassen, die in anderen Organisationen konfiguriert wurden* (in der bereits erwähnten Einstellung *Schreibzugriff auf Wechseldatenträger verweigern, die nicht durch BitLocker geschützt sind*).



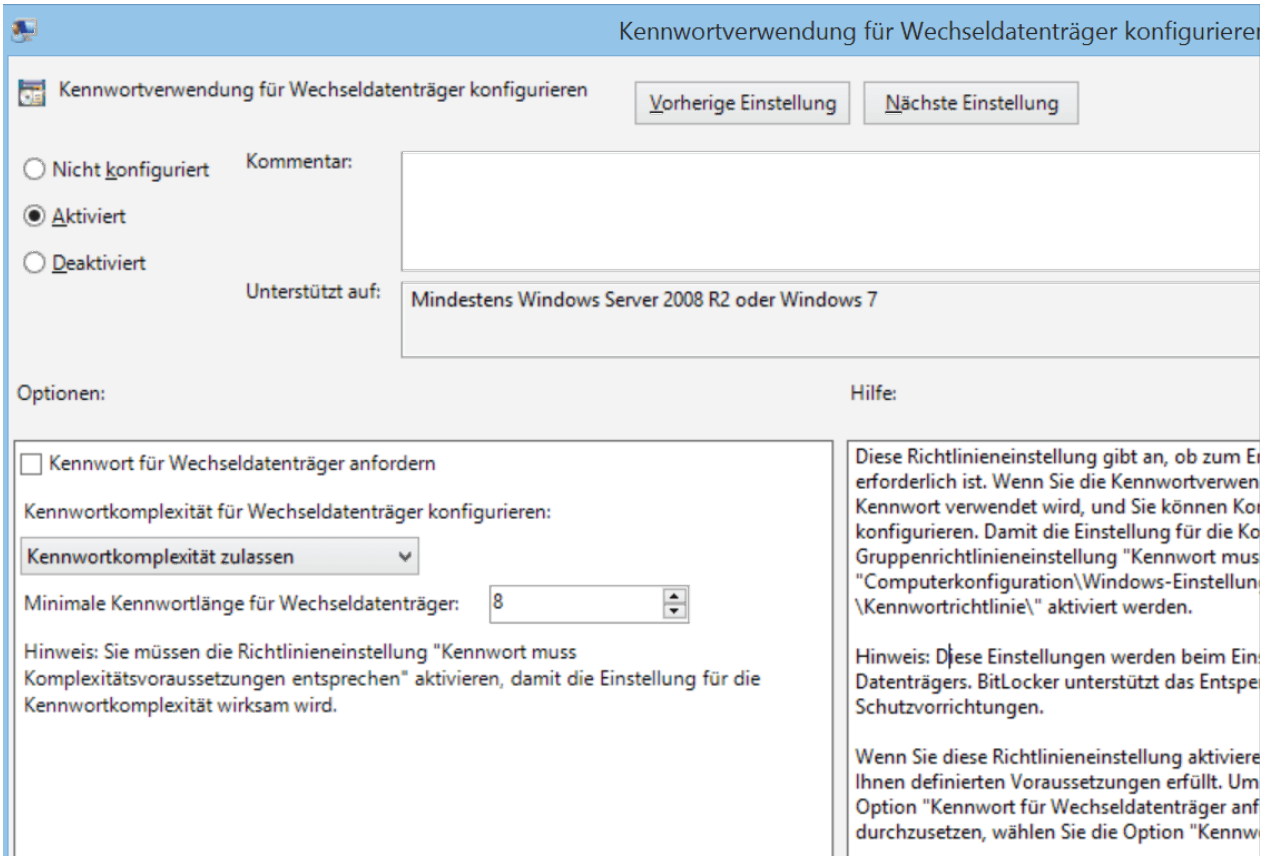
Verhindern, dass Dateien auf Wechseldatenträger geschrieben werden, die nicht mit der eigenen Organisations-ID markiert sind

Neben der eigenen ID kann man weitere, durch Komma getrennte IDs unter *BitLocker-Feld für zulässige IDs* eingeben, um auch die damit gekennzeichneten Geräte zuzulassen.

Passwort-Policy

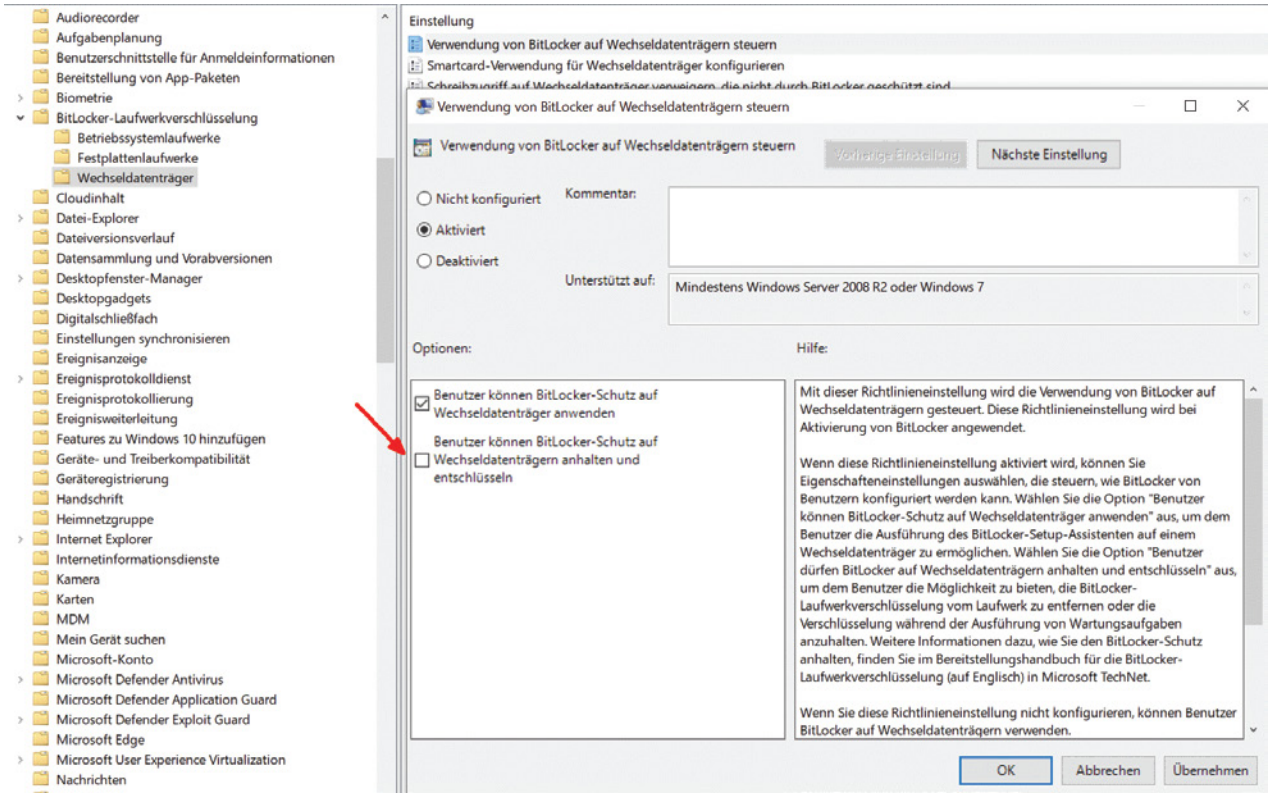
Schließlich kann man für BitLocker To Go eigene Regeln für Passwörter definieren, um beispielsweise die Mindestlänge von standardmäßig acht Zeichen zu erhöhen.

Zuständig dafür ist die Einstellung *Kennwortverwendung für Wechseldatenträger konfigurieren*. Die Komplexitätsanforderung setzt voraus, dass eine Password Policy für die Domäne konfiguriert wurde.



Optionen zur Durchsetzung starker Passwörter für BitLocker To Go

Eine weitere sinnvolle Absicherung von verschlüsselten USB-Laufwerken erhält man über *Verwendung von BitLocker auf Wechseldatenträgern steuern*. Dort sorgt man durch Deaktiveren der Option *Benutzer dürfen BitLocker auf Wechseldatenträgern anhalten und entschlüsseln* dafür, dass die Anwender BitLocker nicht entfernen können.



BitLocker To Go gegen das Deaktivieren durch die Benutzer schützen

Fazit

BitLocker To Go ist das Bordmittel der Wahl, um USB-Datenträger zu verschlüsseln. Ohne zentrale Konfiguration bleibt es aber dem Belieben des Benutzers überlassen, ob und wann er dieses Feature einsetzt. Außerdem obliegt es dann ihm, für die Wiederherstellungsschlüssel aufzubewahren oder die passende Methode zu wählen.

Um einen verlässlichen Schutz der Daten zu gewährleisten, delegieren die meisten Unternehmen diese Aufgaben an die Admins, die entsprechende Vorgaben über die Gruppenrichtlinien durchsetzen können.

Eine völlig transparente und automatische Lösung wird BitLocker To Go aber dadurch nicht. Die zentrale Verwaltung hilft jedoch, die Verwendung des Features deutlich zu vereinfachen.

Datenlaufwerke automatisch entsperren

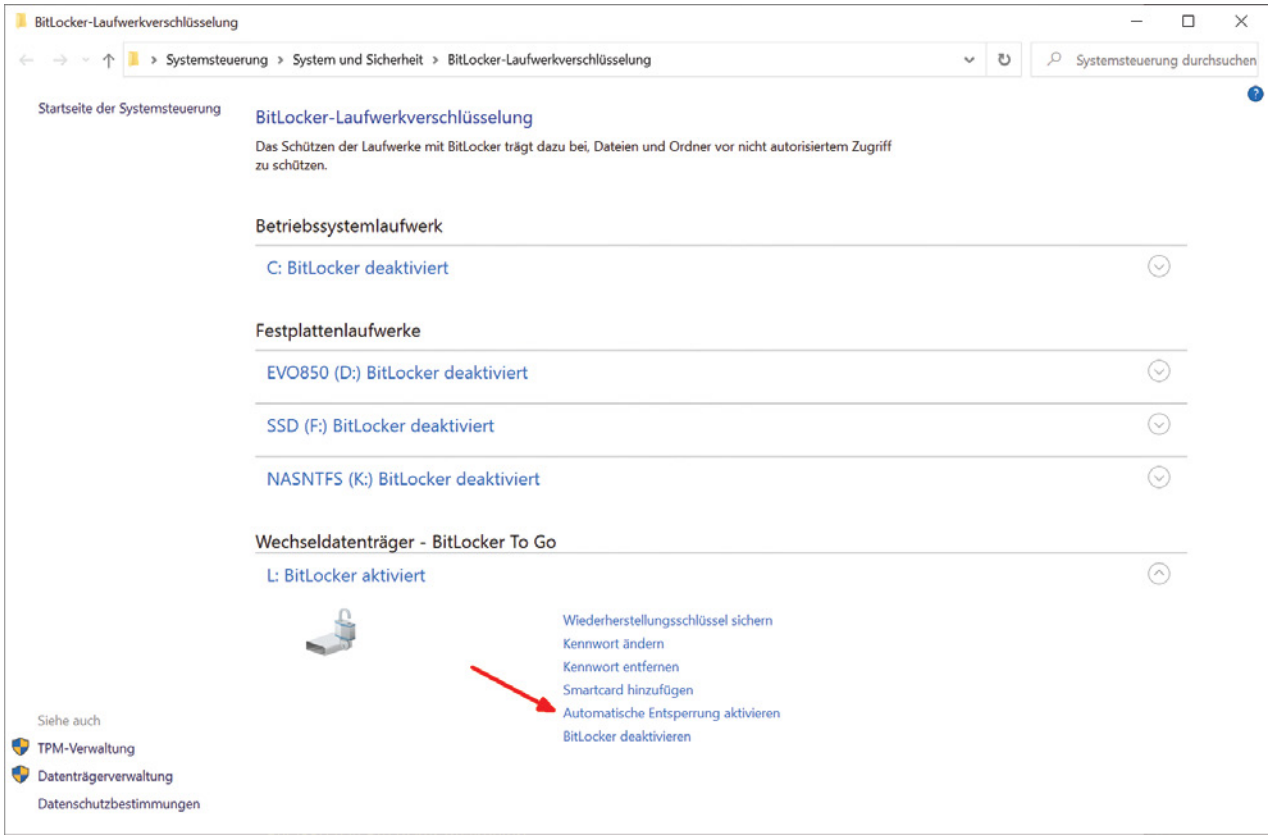
Wenn ein Rechner neben dem System-Volume über Datenlaufwerke verfügt, die mit BitLocker verschlüsselt sind, dann ist es angenehm, wenn man sie nicht immer separat entsperren muss. Das gilt erst recht für Wechseldatenträger. BitLocker bietet mit Auto-Unlock und SID-Protector dafür zwei Verfahren.

Gerade bei BitLocker To Go verwendet man in der Regel Passwörter und Wiederherstellungsschlüssel als Mechanismen zum Entsperren von Datenträgern. Standardmäßig muss man das Kennwort jedes Mal eingeben, sobald man einen verschlüsselten USB-Stick an einen Rechner anschließt.
In einer sicheren Umgebung ist dies meist nicht notwendig, so dass man die Benutzer von dieser lästigen Aufgabe befreien kann. Dies lässt sich durch den Einsatz alternativer Protectors erreichen.

Laufwerk an bestimmten PCs automatisch entsperren

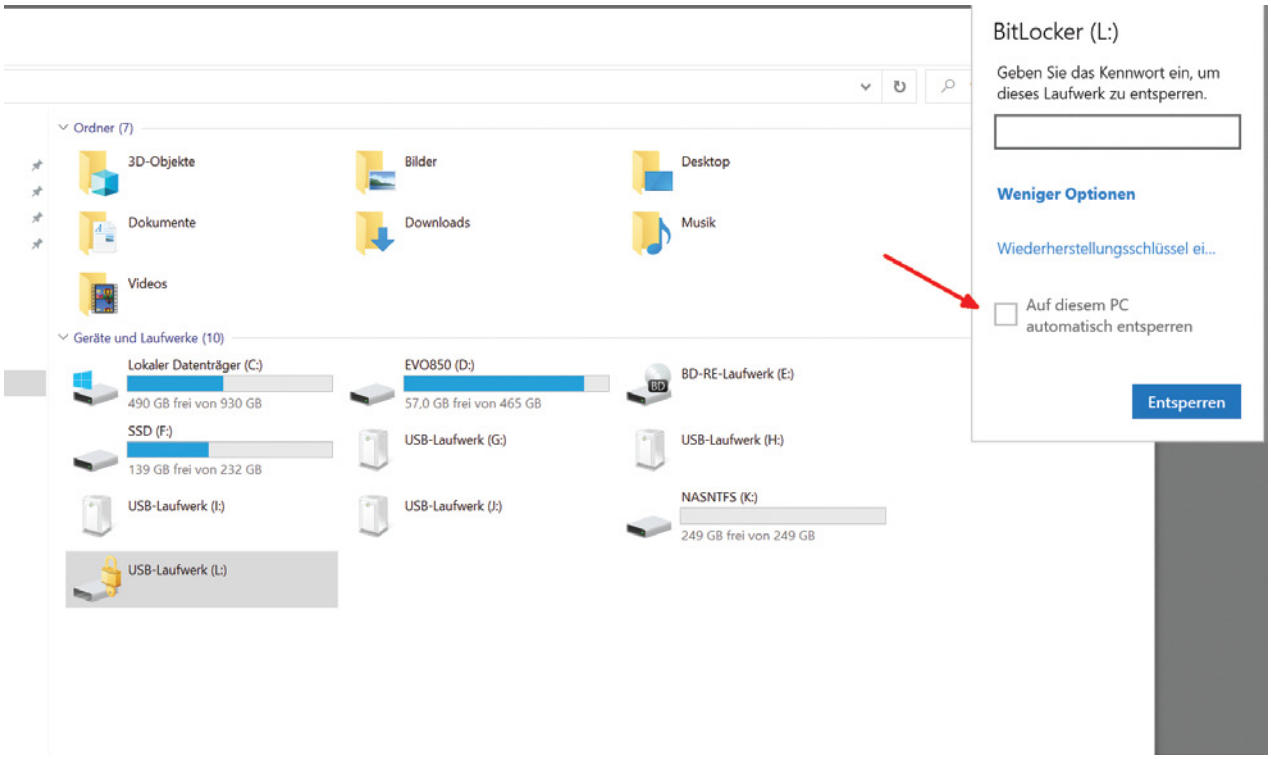
Wenn man möchte, dass ein Datenträger an bestimmten Rechnern ohne Rückfrage entsperrt wird, dann erfüllt das Feature Auto-Unlock diesen Zweck. Es fügt dem Laufwerk einen Protector vom Typ *External Key* hinzu, der Schlüssel wird dabei in der Registry abgelegt.

Anwender können diese Funktion selbst aktivieren, indem sie der Systemsteuerung unter *System und Sicherheit => BitLocker-Laufwerkverschlüsselung* die Details des betreffenden Laufwerks öffnen und dort auf *Automatische Entsperrung aktivieren* klicken. Der Menüeintrag ändert sich dadurch auf *Automatische Entsperrung deaktivieren*, so dass man das Verhalten von BitLocker damit wieder zurücksetzen kann.



Automatische Entsperrung über die Systemsteuerung aktivieren

Alternativ findet sich die Möglichkeit zum Aktivieren der automatischen Entsperrung im Kennwort-Dialog, der sich nach dem Zugriff auf den verschlüsselten Datenträger öffnet. Dort kann man unter *Mehr Optionen* die zuständige Checkbox anhaken.



Benutzer können gleich bei der Abfrage des Passworts die automatische Entsperrung konfigurieren

Während man diese Einstellung auf der GUI ohne administrative Rechte ändern kann, benötigen die Pendants auf der Kommandozeile erhöhte Privilegien. Das betrifft sowohl

manage-bde -autounlock -enable <Laufwerksbuchstabe>

als auch das PowerShell-Cmdlet

Enable-BitLockerAutoUnlock -MountPoint <Laufwerksbuchstabe>

Für die gegenteilige Operation sind *manage-bde -autounlock -disable* bzw. *Disable-BitLockerAutoUnlock* zuständig.

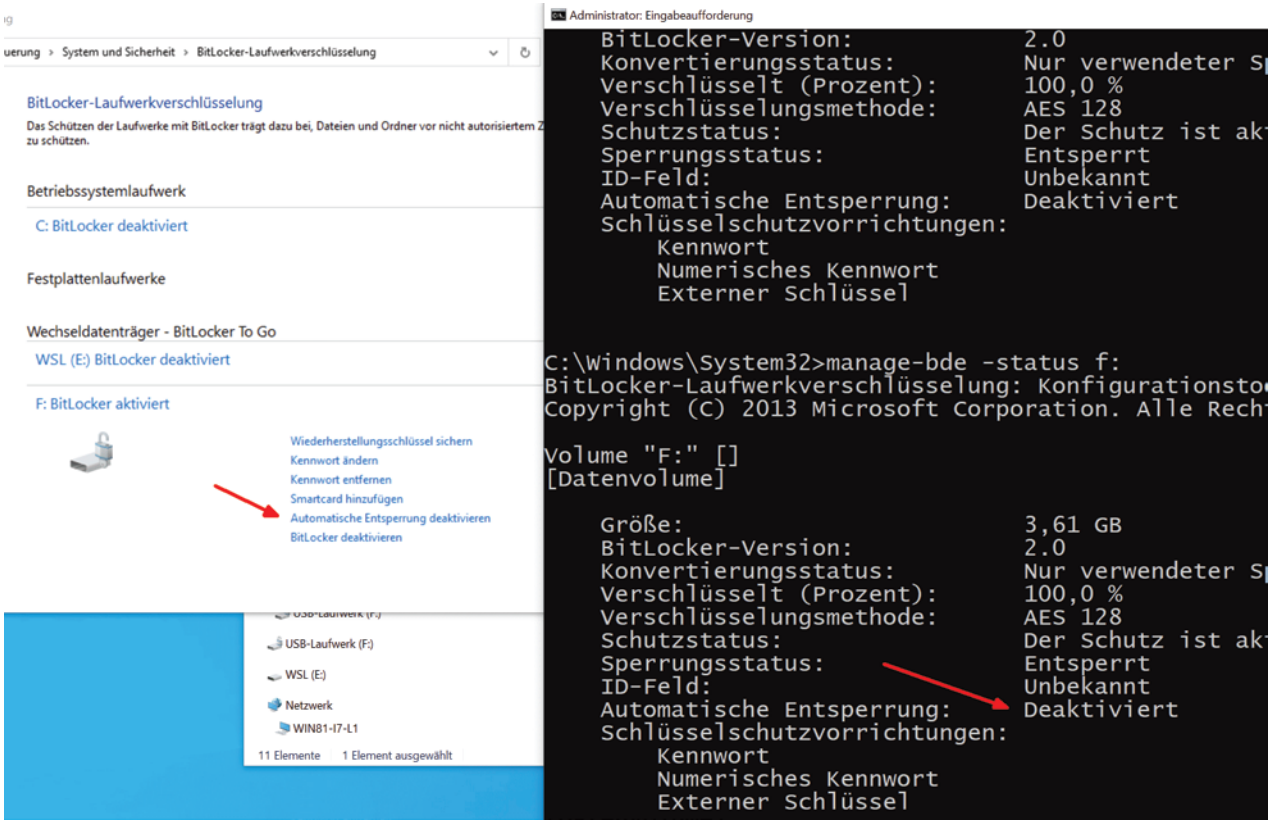
Dieses unterschiedliche Verhalten führt zu Inkonsistenzen. So melden weder

manage-bde -status <Laufwerksbuchstabe>

noch

Get-BitLockerVolume -MountPoint <Laufwerksbuchstabe>

die automatische Entsperrung als aktiv, wenn man sie als Standardbenutzer über die GUI eingeschaltet hat, weil sie nur pro Konto gilt.



Die Kommandozeilen-Tools erkennen nicht, dass ein Standard-User die automatische Entsperrung aktiviert hat

Als Admin kann man sich die von anderen Benutzern konfigurierte automatische Entsperrung mit

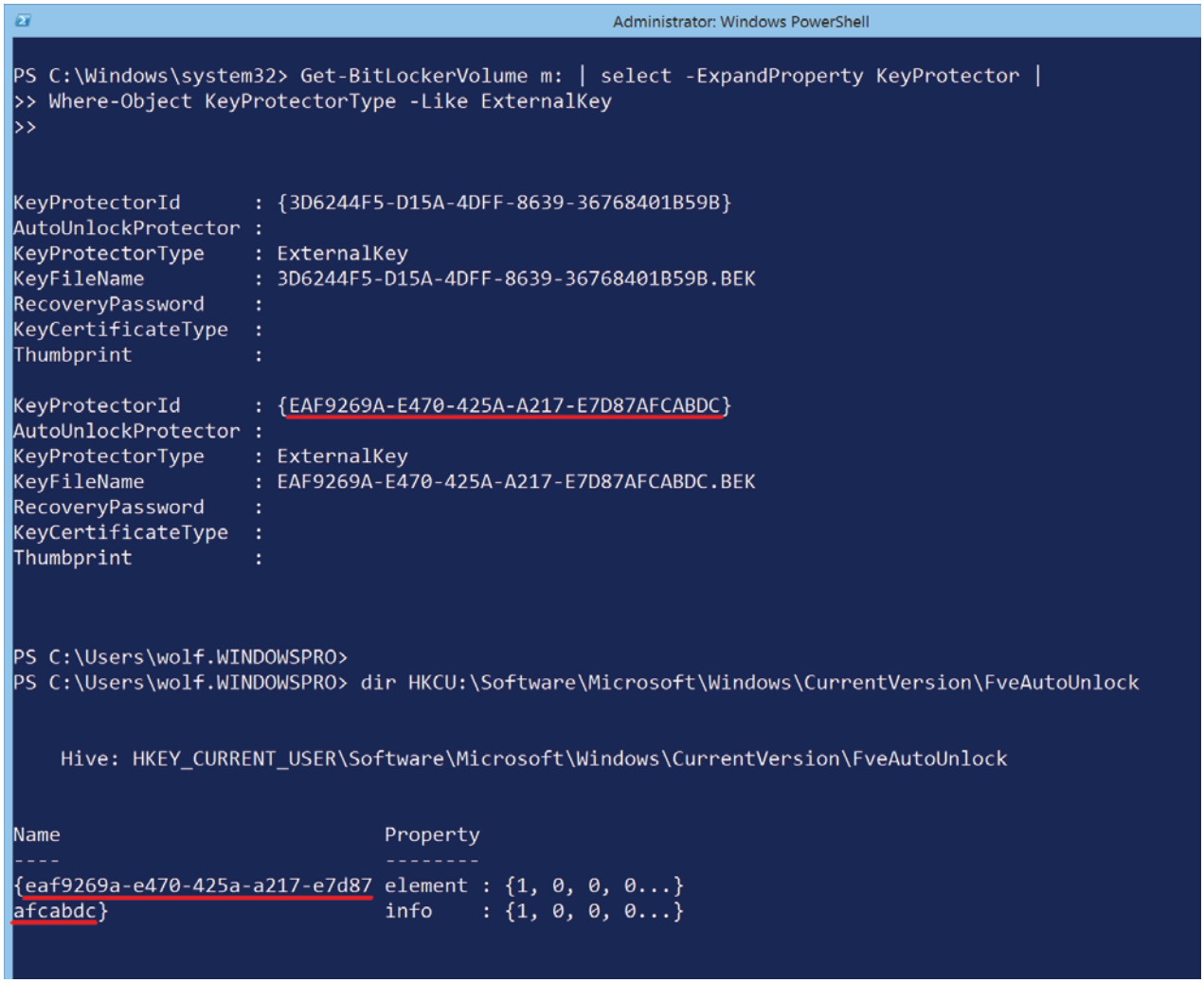
manage-bde -protectors -get <Laufwerksbuchstabe> -Type ExternalKey

anzeigen lassen. *Get-BitLockerVolume* liefert die entsprechenden Schlüssel über die Eigenschaft *KeyProtector*.

Die Tools lesen dazu den Eintrag im Hive für Current User unter

HKCU:\Software\Microsoft\Windows\CurrentVersion\FveAutoUnlock

aus.



Die ID des Protectors entspricht dem Schlüssel in der Registrierdatenbank

Welcher Schlüssel welchem Benutzer zugeordnet ist, kann man daraus aber nicht entnehmen. Die Eigenschaft *AutoUnlockProtector* zeigt nämlich nur für den eigenen Schlüssel den Wert *True*.

Laufwerk für AD-Benutzer entsperren

Möchte man verschlüsselte Wechseldatenträger, die häufig an verschiedene PCs angeschlossen werden, für bestimmte Benutzer unabhängig vom jeweiligen Rechner freischalten, dann erreicht man das über einen Protector vom Typ *AdAccountOrGroup*.

Auf diese Weise kann man User etwa mit einem personalisierten USB-Stick ausstatten, den nur sie lesen dürfen und den sie nicht extra entsperren müssen, solange sie an der Domäne angemeldet sind.

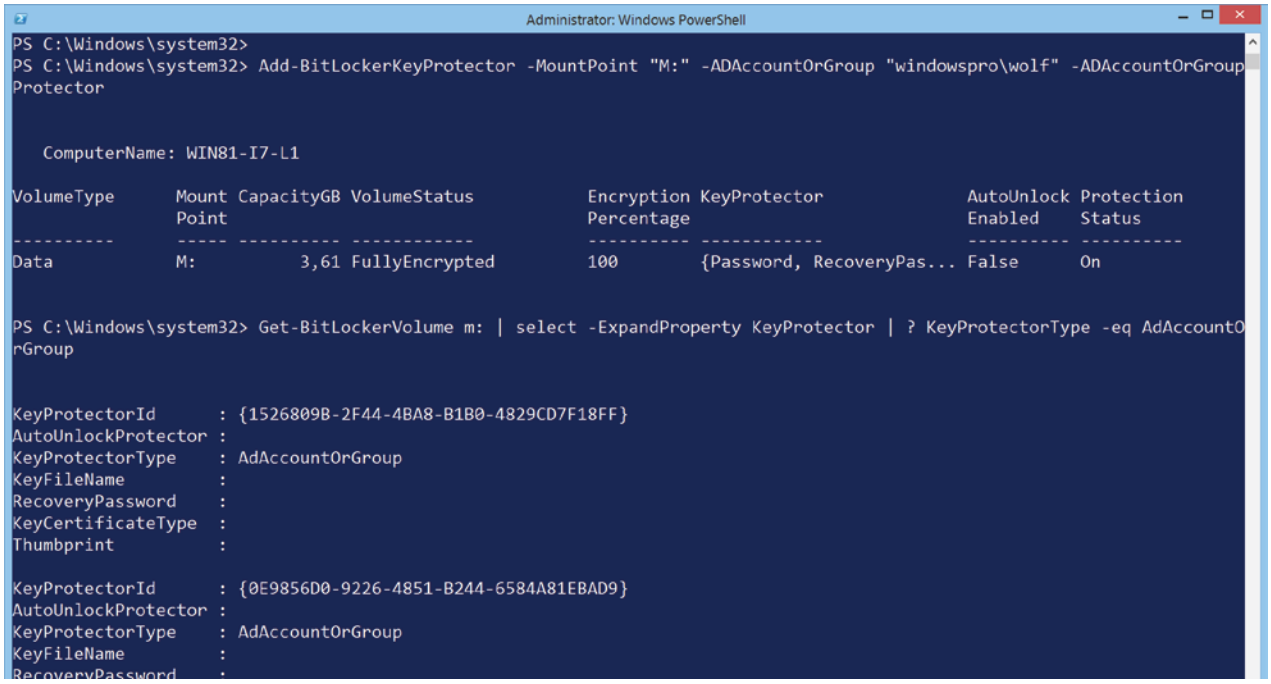
Auf ihren privaten Geräten können sie solche Datenträger aber nicht entschlüsseln, zumindest solange sie nicht Zugang zu einem anderen Mechanismus wie Passwörter oder Wiederherstellungsschlüssel haben.

Um einen solchen Protector hinzuzufügen, benötigt man erhöhte Rechte, so dass in der Regel die IT-Abteilung solche USB-Datenträger bereitstellen wird. Die zuständigen Tools dafür sind wieder manage-bde oder PowerShell:

manage-bde -protectors -add <Laufwerksbuchstabe> -sid DOMAIN\user

Das BitLocker-Modul von PowerShell sieht dafür folgendes Cmdlet vor:

Add-BitLockerKeyProtector -MountPoint <Laufwerksbuchstabe> `
-ADAccountOrGroup "DOMAIN\user" -ADAccountOrGroupProtector



SID-Protector über PowerShell hinzufügen

Wenn man PowerShell zum Aktivieren von BitLocker einsetzt, dann kann man bereits *Enable-BitLocker* die beiden Parameter *ADAccountOrGroup* und *ADAccountOrGroupProtector* mitgeben.

Wie man aus deren Namen erkennt, akzeptiert der Aufruf nicht nur einzelne AD-Accounts, sondern auch Benutzergruppen. Theoretisch könnte man damit Medien mit *DOMAIN\Domänen-Benutzer* so präparieren, dass alle Anwender im Unternehmen damit arbeiten können, aber die Daten für alle unzugänglich bleiben, sobald sie nicht an der Domäne angemeldet sind.

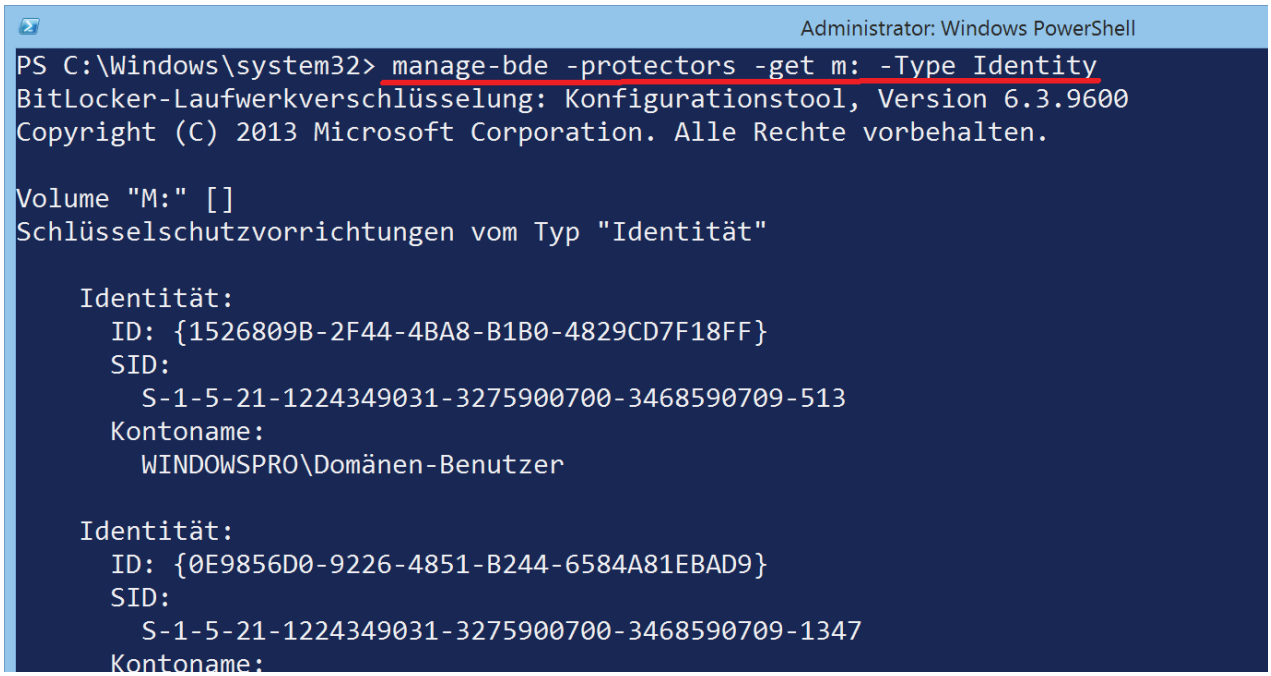
Wenn man wissen möchte, ob ein solcher Protector für einen Datenträger konfiguriert wurde, dann findet man das so heraus:

```
Get-BitLockerVolume <Laufwerksbuchstabe> | select -ExpandProperty KeyProtector |
where KeyProtectorType -eq AdAccountOrGroup
```

Alternativ zeigt auch

```
manage-bde -protectors -get <Laufwerksbuchstabe> -Type Identity
```

diese unter der Bezeichnung *Schlüsselschutzvorrichtungen* an.



SID-Protectors (Typ Identity) mit Hilfe von manage-bde ausgeben

Entfernen kann man sie mit Hilfe von Remove-BitLockerKeyProtector.

Vor- und Nachteile

Bei Auto-Unlock und SID-Protector handelt es sich mithin um Komfortfunktionen für BitLocker, die Benutzern in sicheren Umgebungen das laufende Eingeben von Passwörtern ersparen. Erstere entsperrt verschlüsselte Datenträger für den aktuellen User auf einem bestimmten Rechner, Zweitere für ausgewählte Benutzer oder Gruppen auf allen PCs, solange sie an der Domäne angemeldet sind.

Leider lässt die Umsetzung dieser Funktionen einige Wünsche offen. So gibt es bei Auto-Unlock Inkonsistenzen zwischen den CLI-Tools und der GUI-Option in der Systemsteuerung. Hinzu kommt, dass sich beide nicht über Gruppenrichtlinien verwalten lassen, sondern dass Admins für ein zentrales Management auf PowerShell oder manage-bde.exe angewiesen sind.

BitLocker zentral mit ACMP von Aagon verwalten

Das Management von BitLocker mittels Scripts oder GPOs leidet unter einigen Einschränkungen. So können Admins nicht ohne weiteres erkennen, ob die Verschlüsselung aus einem der vielen möglichen Gründe gescheitert ist und daher mehrere PCs ungeschützt sind.

Neben dem fehlenden Reporting besteht ein weiteres Defizit in der relativ unflexiblen Zuweisung der Einstellungen, wenn man dafür die Gruppenrichtlinien verwendet. Wenn man nicht ganze OUs oder Domains mit den gleichen BitLocker-Optionen konfigurieren will, muss man mit WMI-Filtern hantieren. Nicht zuletzt stellt das zentrale Aktivieren von BitLocker eine gewisse Herausforderung dar, weil die Gruppenrichtlinien dafür keine Einstellung bieten. Wer nur mit den Bordmitteln arbeitet, muss dafür auf Scripts zurückgreifen.

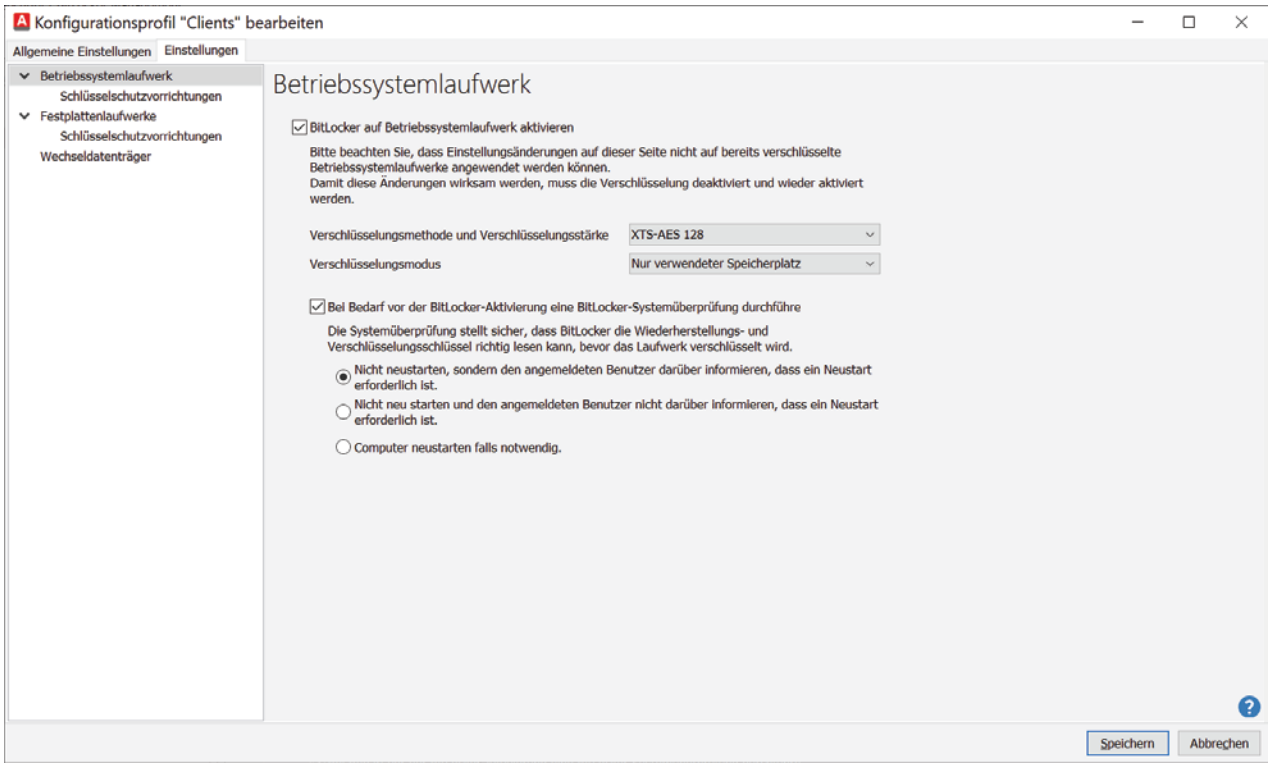
BitLocker-Verwaltung als Funktion des Client-Managements

Bei ACMP hingegen handelt es sich um eine umfassende Lösung für das Endpoint-Management, dessen Infrastruktur auch der BitLocker-Verwaltung zugute kommt. So verfügt es bereits über ein vollständiges Inventar aller Rechner, das Admins gezielt für die Konfiguration von BitLocker verwenden können.
Zudem besitzt ACMP eine Reporting-Komponente, die auch über den Verschlüsselungsstatus der PC-Laufwerke Auskunft geben kann. Schließlich nutzt das System auf jedem Client einen Agent, der unter anderem auch die Verschlüsselung der Laufwerke anstoßen kann, ohne dass Admins dafür ein separates Script starten oder den Benutzer um Mithilfe bitten müssen.

BitLocker-Konfiguration über Profile

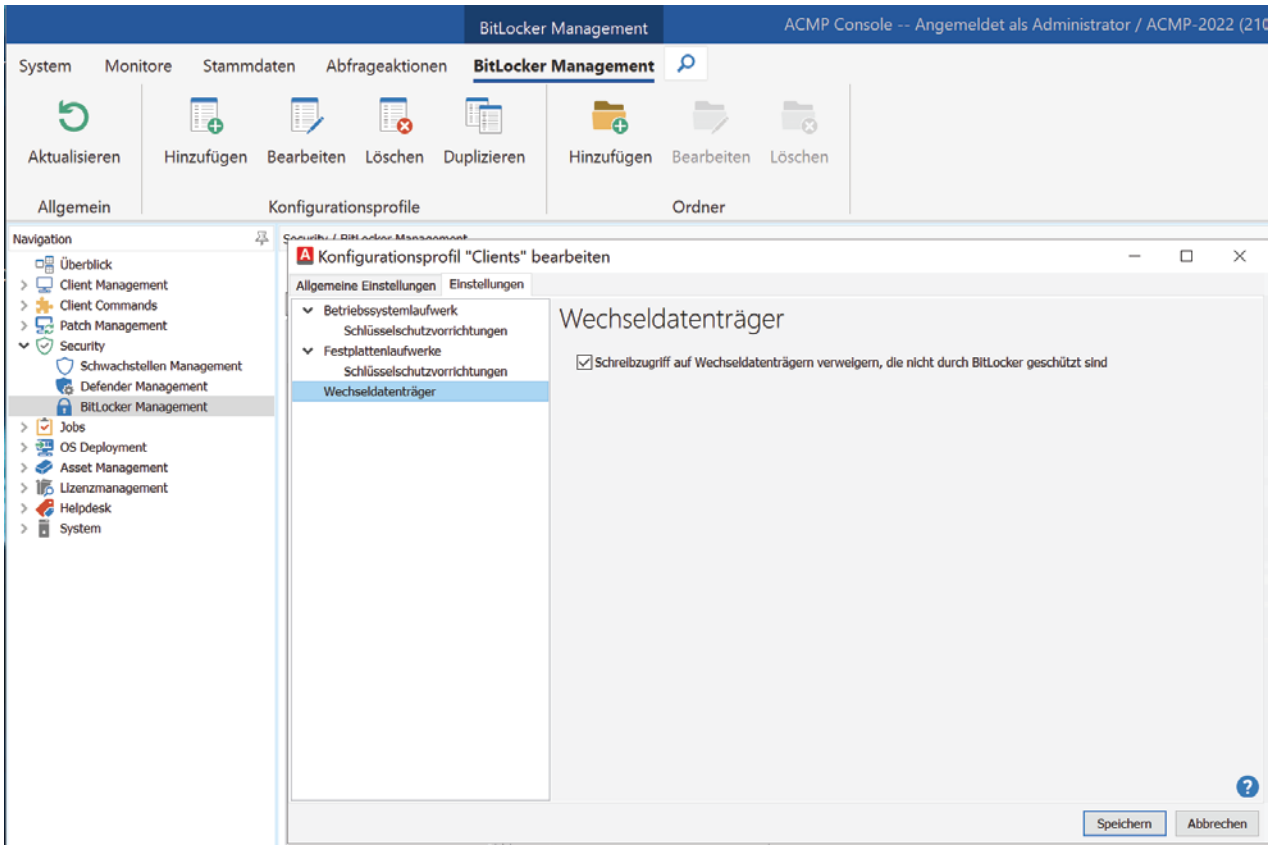
ACMP fasst alle BitLocker-Einstellungen in Profilen zusammen. Per Voreinstellung enthält ACMP die Profile *Clients* und *Server*, aber Admins können beliebig viele eigene Profile mit jeweils verschiedenen Einstellungen anlegen.

Diese enthalten sowohl die Konfiguration für das System- als auch für Datenlaufwerke. Zur Auswahl stehen dort etwa die Verschlüsselungsmethode, die Optionen zum Reboot des Rechners vor dem Start der Verschlüsselung, die Anforderungen an eine PIN bzw. an ein Passwort oder das automatische Entsperren.



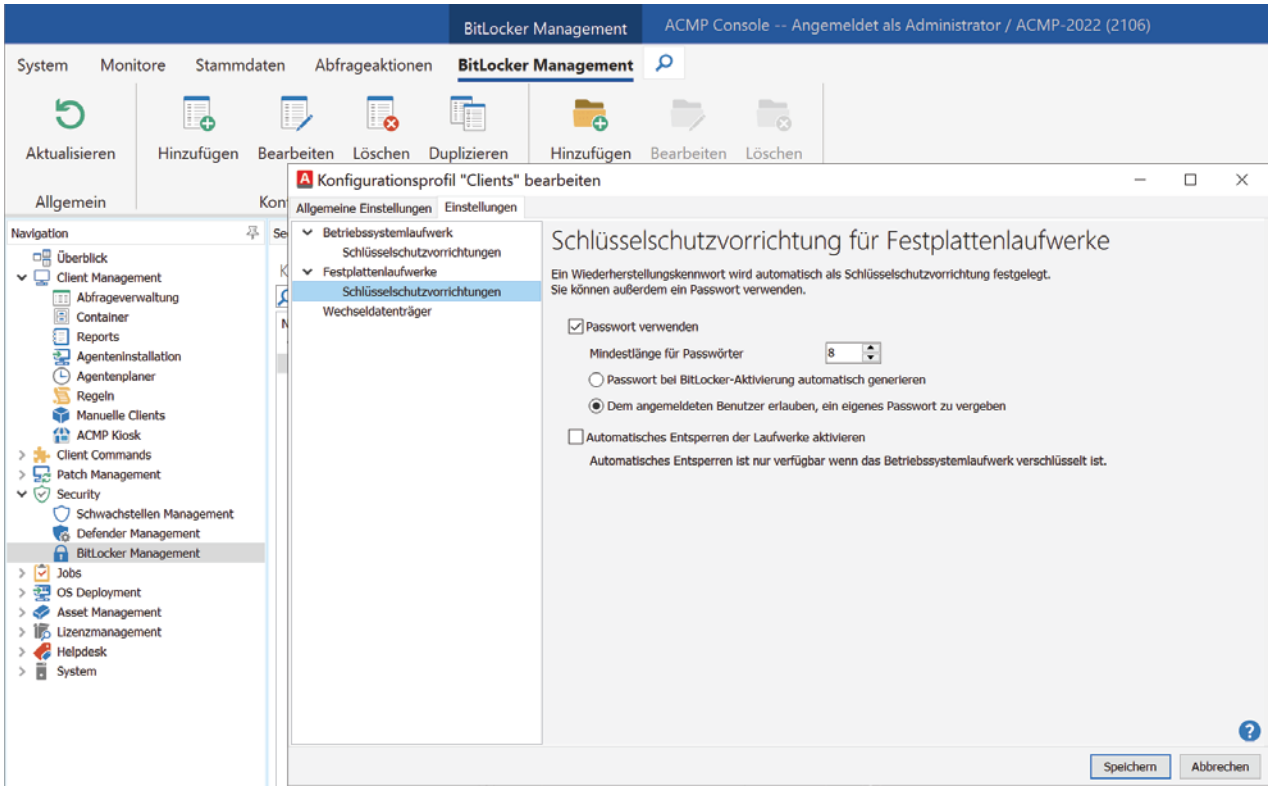
ACMP BitLocker Management-Einstellungen für das Systemlaufwerk im Profil für Clients

Unter *Wechseldatenträger* findet sich für BitLocker ToGo nur eine Einstellung, nämlich jene, die den Zugriff auf unverschlüsselte Speichergeräte verhindert. Die Benutzer sind damit gezwungen, nur Datenträger zu verwenden, die von ihnen oder der IT-Abteilung zuvor verschlüsselt wurden.



Die Unterstützung für BitLocker ToGo besteht im Zwang zur Nutzung verschlüsselter Datenträger

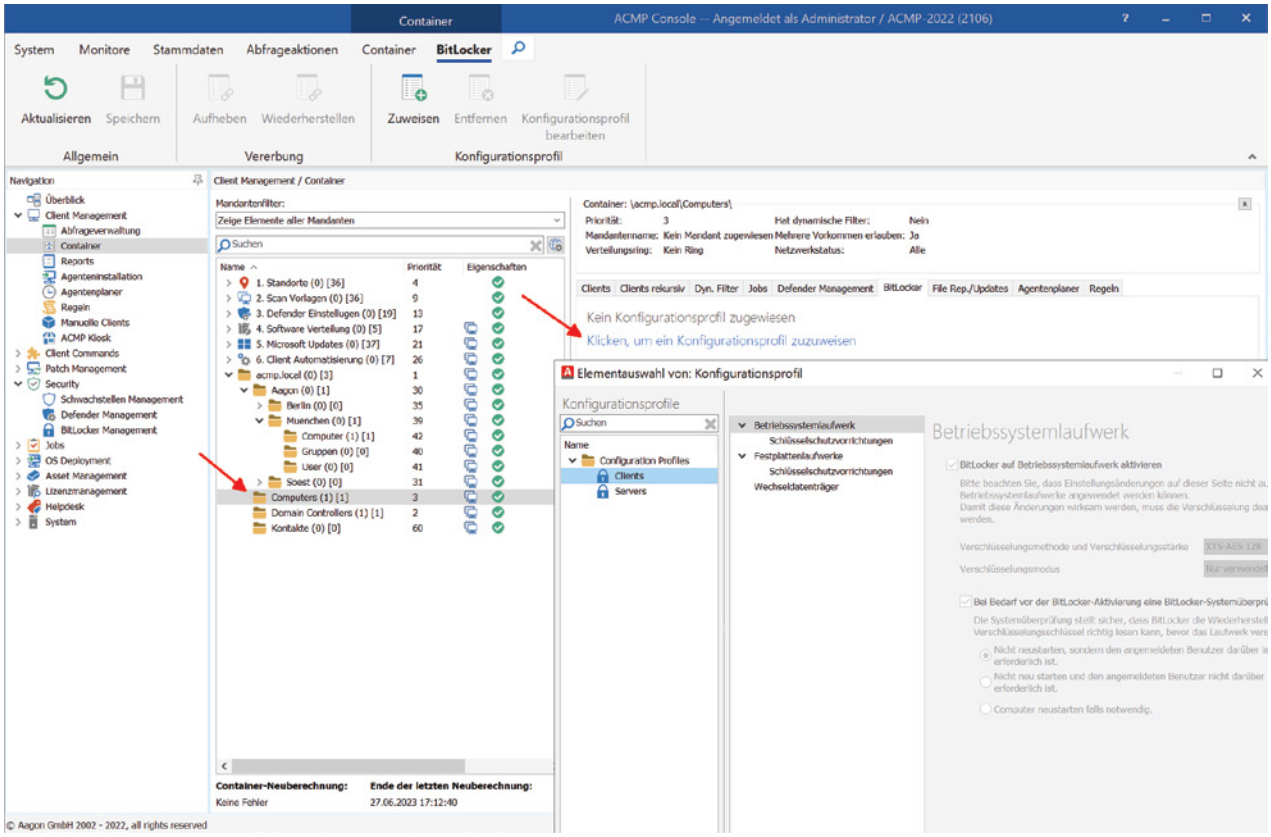
Mit Hilfe der Profile können Admins den Rechnern dann ein ganzes Paket an Einstellungen auf einmal zuweisen. Dies funktioniert ähnlich wie mit GPOs, die mehrere Richtlinien enthalten.



Einstellungen für Datenlaufwerke in einem Konfigurationsprofil des ACMP BitLocker Management

Profile an Endgeräte zuweisen

Allerdings erweist sich ACMP dabei im Vergleich zu den Gruppenrichtlinien als wesentlich flexibler. Als Ziel kommen nicht nur OUs in Frage, sondern auch Container, deren Inhalt dynamisch über Abfragen anhand fast beliebiger Kriterien erzeugt wird.

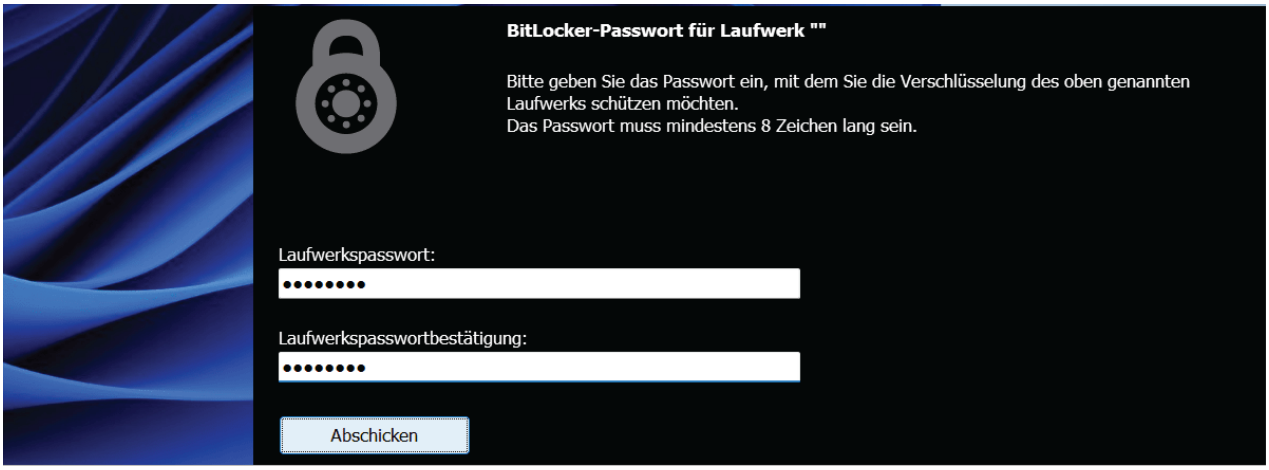


Konfigurationsprofil an einen ACMP-Container zuweisen

Alternativ ist aber auch möglich, ein Profil einem einzelnen Rechner zuzuweisen, beispielsweise für das Testen eines Profils.

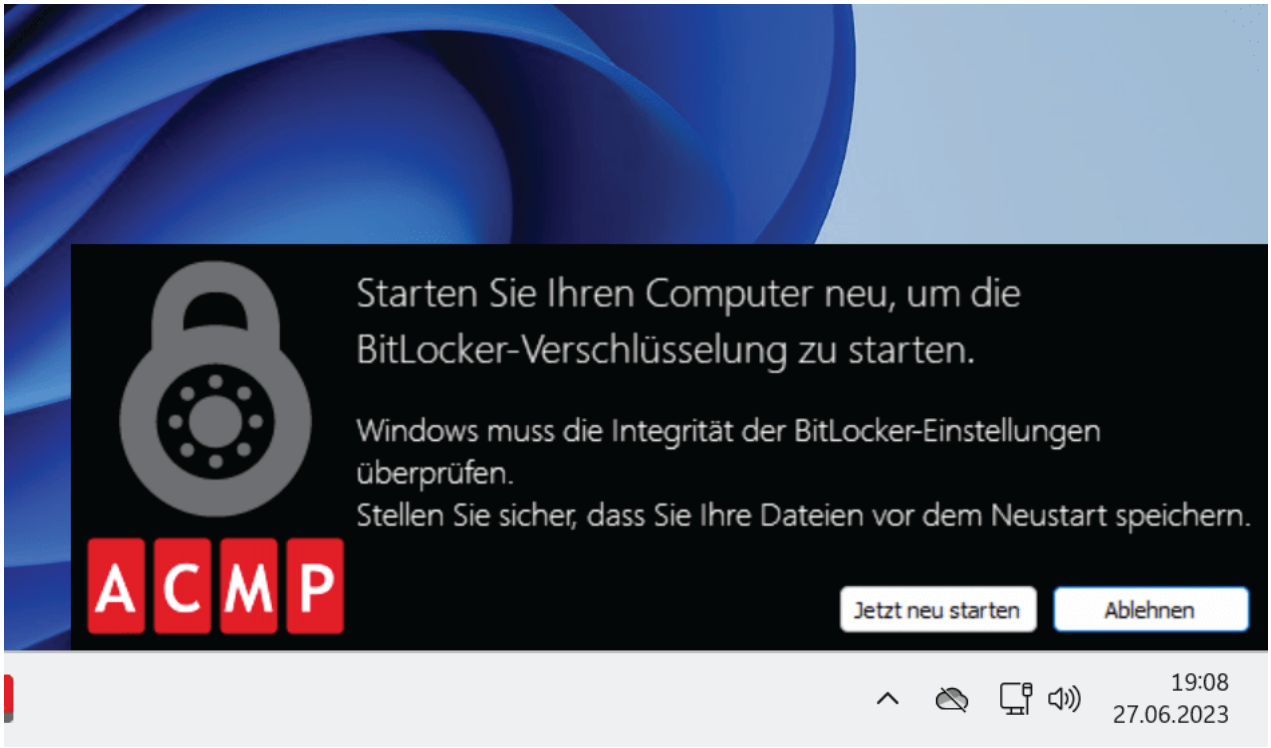
Verschlüsselung starten

Die Zuweisung eines BitLocker-Profils zu einem oder mehreren Geräten bewirkt, dass dort die Verschlüsselung sofort beginnt. Im ersten Schritt muss der Benutzer, falls das Profil die Verwendung einer PIN vorsieht, diese festlegen.



Die BitLocker-Verschlüsselung startet mit der Vergabe einer PIN, wenn diese gewollt ist

Anschließend muss der PC neu starten, und dies geschieht abhängig von den gewählten Optionen entweder automatisch oder dadurch, dass die Benutzer die entsprechende Anfrage bestätigen.

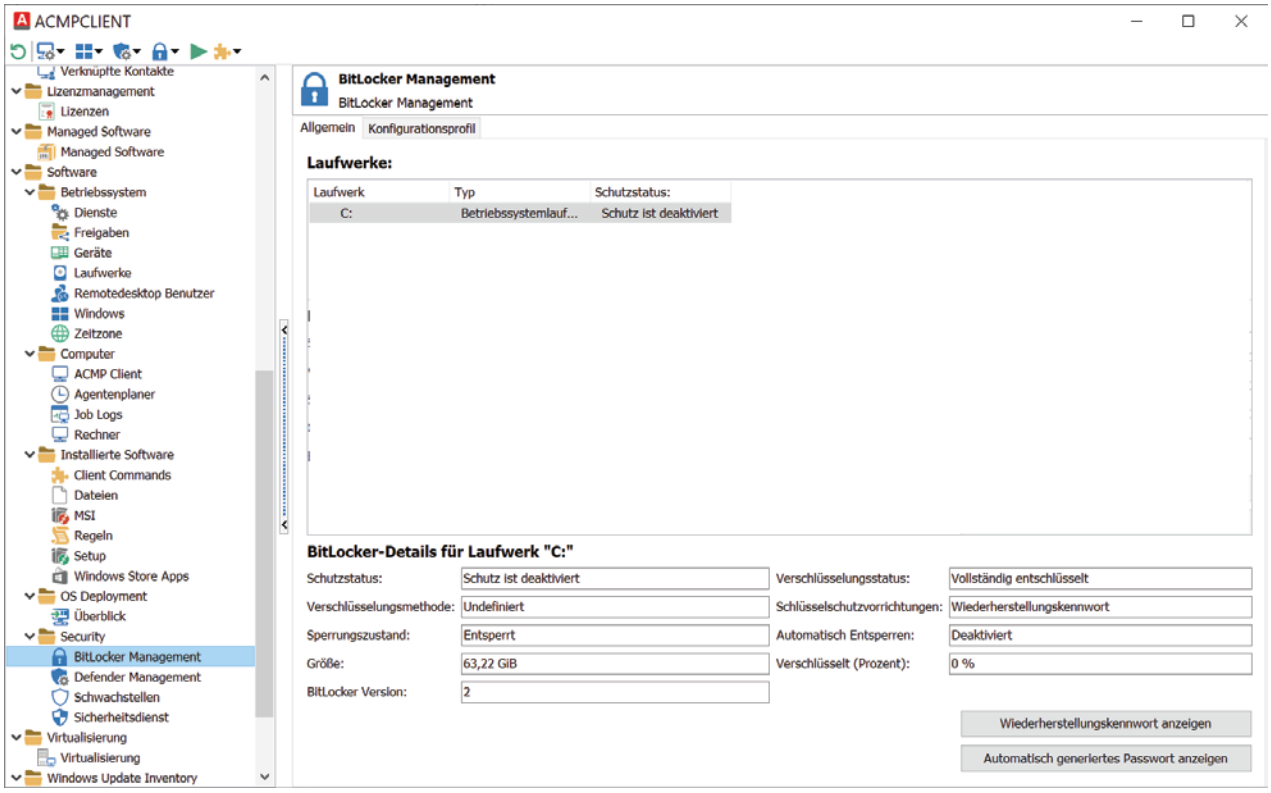


Vor dem Beginn der Verschlüsselung überprüft BitLocker die Integrität des Systems

Nachdem der Rechner wieder hochgefahren ist, sollte nach der eventuell nötigen Eingabe der PIN die Verschlüsselung im Hintergrund beginnen. Sie betrifft je nach Auswahl im Profil das gesamte Laufwerk oder nur den belegten Speicherplatz.

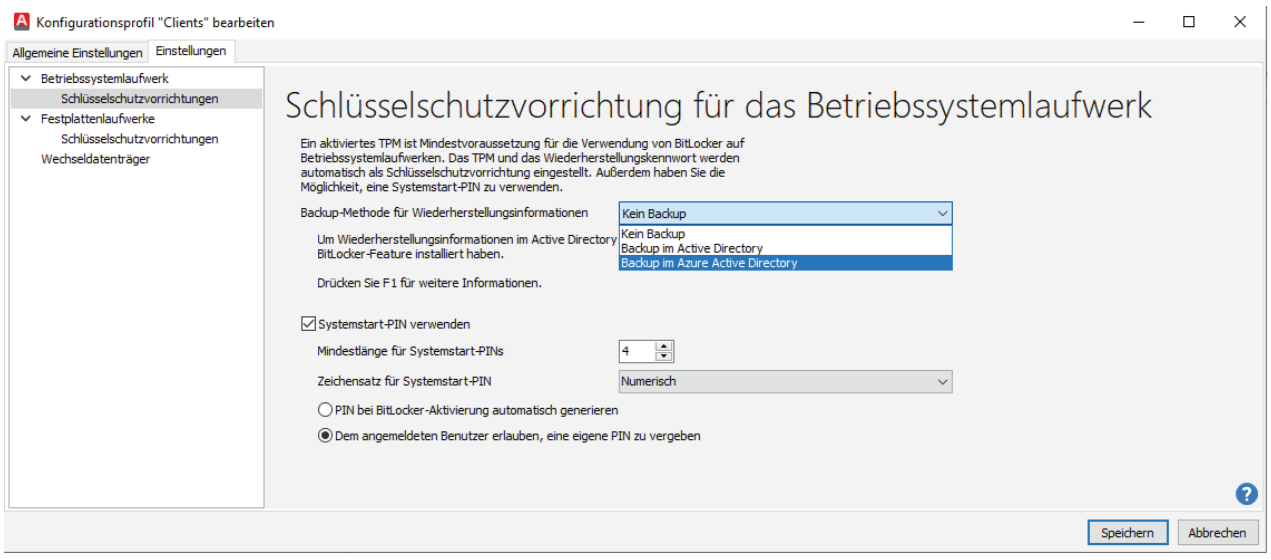
Verwaltung der Passwörter

ACMP legt das Passwort für die Wiederherstellung verschlüsselt in seiner Datenbank ab. Von dort können es Admins in der Konsole bei der Detailansicht eines Clients auslesen.



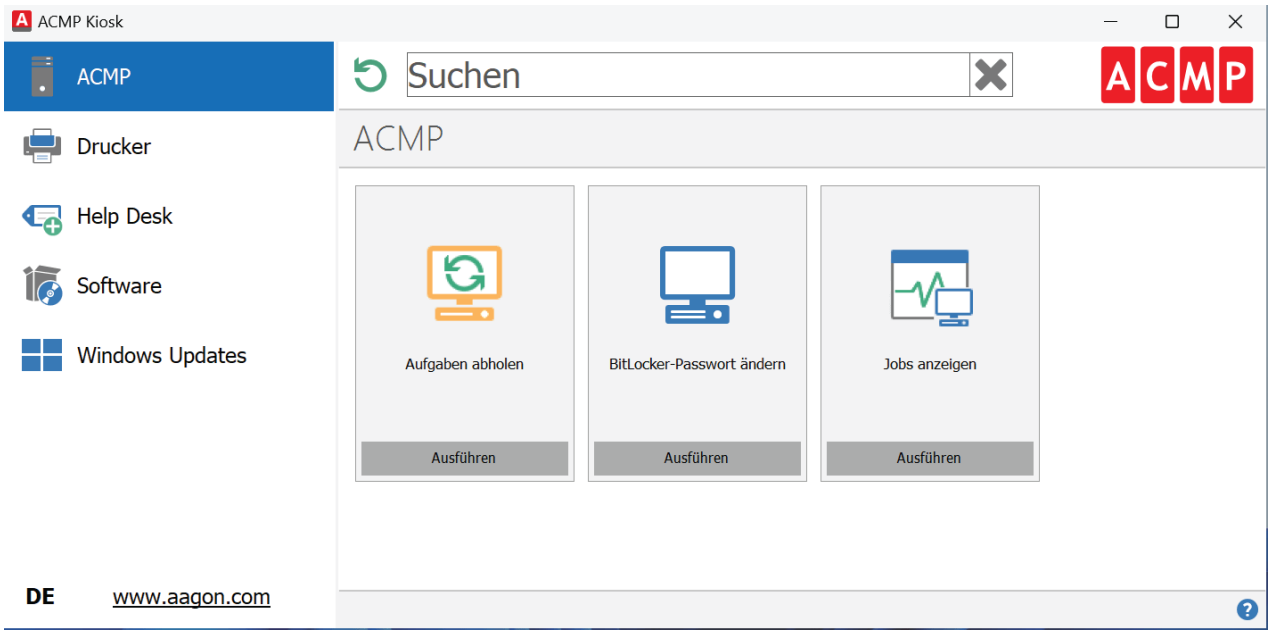
In den Client-Details können Admins das Passwort für die Wiederherstellung auslesen

In der vor kurzem erschienenen Version 6.5 erlaubt ACMP das zusätzliche Speichern des Wiederherstellungspassworts im Active Directory oder in Azure AD. Von dort kann es mit den Bordmitteln durch berechtigte Benutzer ausgelesen werden.



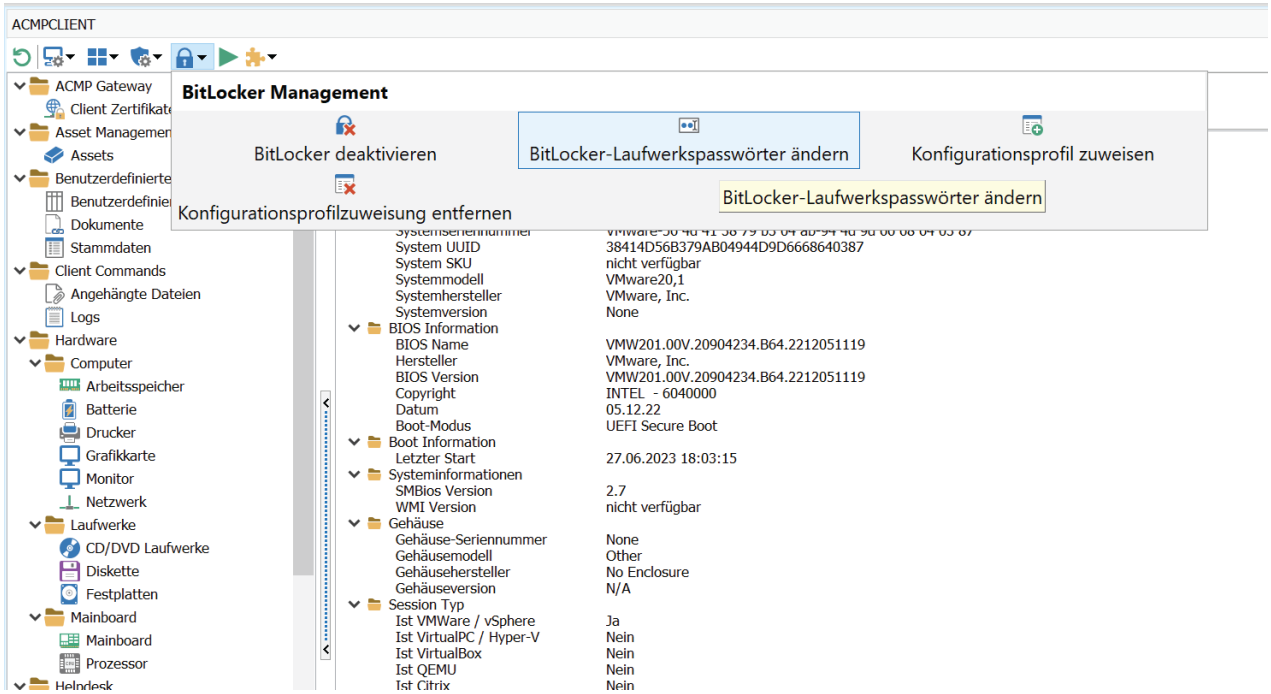
Backup-Option für das Wiederherstellungspasswort in ACMP 6.5

Darüber hinaus können Benutzer das zu Beginn der Verschlüsselung gewählte Passwort später jederzeit ändern. Dafür steht im ACMP Kiosk, einem Bestandteil der Client-Komponente, eine Self-Service-Option zur Verfügung.



Benutzer können das BitLocker-Passwort selbständig über den Kiosk ändern

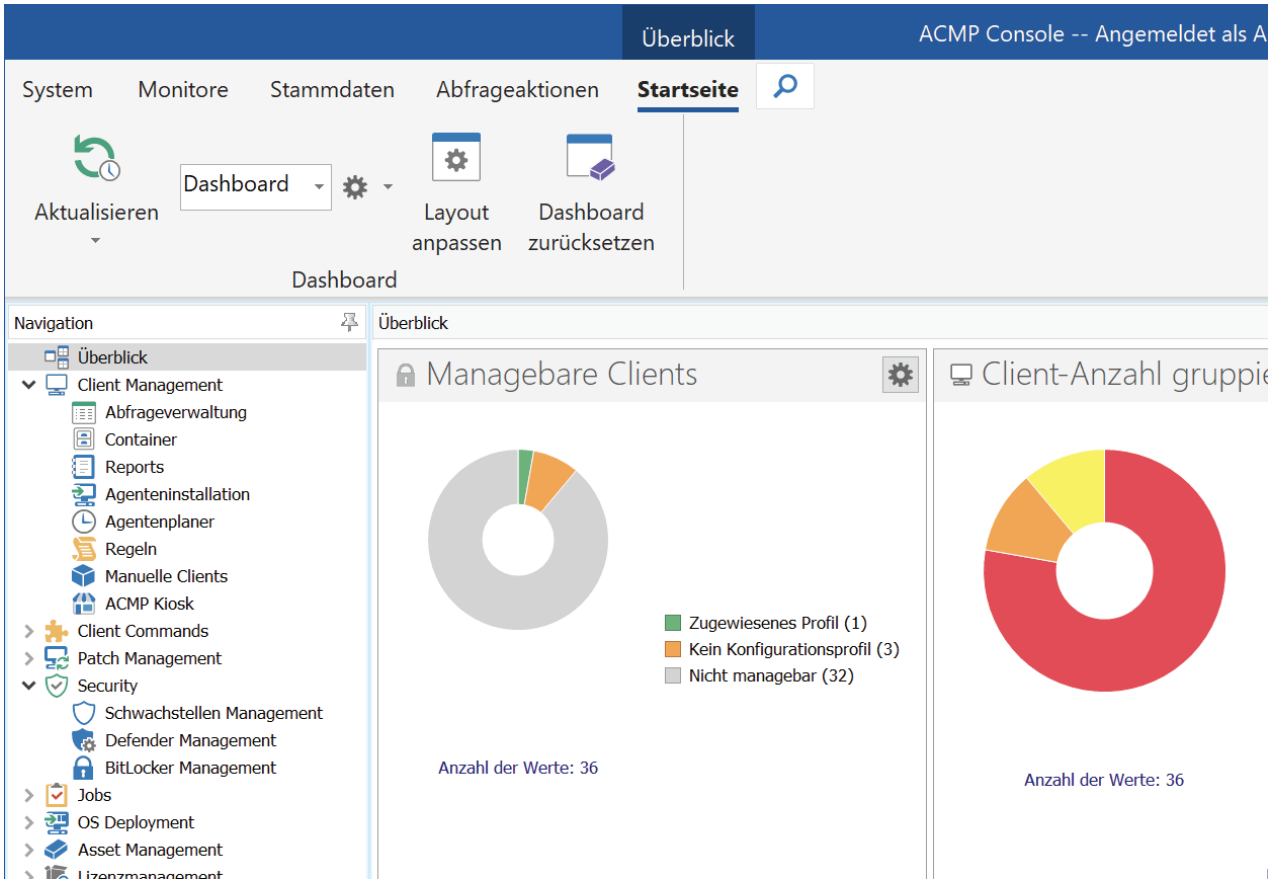
Alternativ lässt sich ein Passwort in der Konsole zurücksetzen. Die Benutzer vergeben dann am Client ein neues Kennwort, ohne dass sie dafür das alte kennen müssen.



BitLocker-Passwort über die Admin-Konsole zurücksetzen

Dashboard und Abfragen

Admins erhalten einen Überblick über den BitLocker-Status auf den Clients, indem sie entsprechende Widgets in das Dashboard einbinden oder vorkonfigurierte sowie selbst formulierte Abfragen ausführen.



Ein ACMP BitLocker Management-Widget zeigt, wie vielen Clients ein Profil zugewiesen wurde

Das Dashboard bietet zwei Widgets zu BitLocker. Das eine zeigt an, welche Clients sich über ACMP verwalten lassen und welche davon bereits ein Profil erhalten haben. Das zweite gibt Aufschluss darüber, welchen Clients welches Profil zugewiesen wurde.

Schließlich kann man sehr schnell über entsprechende Abfragen ermitteln, auf welchen PCs BitLocker durch ACMP verwaltet wird, auf welchen Geräten das Systemlaufwerk nicht verschlüsselt ist und mit welcher Methode die Laufwerke verschlüsselt wurden.

Zusammenfassung

ACMP bietet ein BitLocker Management, das sich die Möglichkeiten einer umfassenden Client-Management-Lösung zunutze macht. Dazu gehört eine zentrale Konsole, aus der Admins nicht nur die Verschlüsselung steuern, sondern auch Reports zum BitLocker-Status in der gesamten Umgebung abrufen können.

Als besonders flexibel erweist sich die Kombination aus Konfigurationsprofilen und dynamisch erzeugten Containern für die Zuweisung der gewünschten Einstellungen zu ausgewählten Geräten. Sobald PCs ein Profil erhalten haben, veranlasst der Agent die sofortige Verschlüsselung.

BitLocker aktiviert aus verschiedensten Gründen den Recovery Mode, welcher die Eingabe des Wiederherstellungsschlüssels erfordert. ACMP speichert diesen in seiner Datenbank, aus der er über die Admin-Konsole unkompliziert ausgelesen werden kann. Zudem bietet die aktuelle Version eine Backup-Option für das Active Directory.

Verfügbarkeit

Die Aagon GmbH bietet eine kostenlose ACMP Testversion inklusive des BitLocker Managements auf ihrer Website an.

ÜBER AAGON

„Manage any device in a connected world!" – Aagon entwickelt seit 30 Jahren Client-Management- und -Automation-Lösungen und ist der Spezialist für die Verwaltung von Endgeräten und die Automatisierung von Standardaufgaben. Durch sorgfältige Entwicklungen, mehr als 20 Jahre Marktreife und die enge Zusammenarbeit mit unseren Kunden und Partnern sind unsere Produkte perfekt auf Ihre Anforderungen und Bedürfnisse zugeschnitten.

Individuelle Beratung und die beste Unterstützung von Kunden und Partnern bei der Installation und ersten Einrichtung gehören deshalb zum Standard von Aagon. Ein umfassendes Verständnis von Kundenbedürfnissen und der ständige Kontakt zu unseren Kunden und Partnern ermöglichen Softwareentwicklung auf Augenhöhe.

Webinare-on-Demand, zahlreiche Whitepaper und die beliebten Treffen zum Anwendertreffen an Standorten in ganz Deutschland sind nur drei Beispiele, wie nahe am Kunden ACMP wirklich entwickelt wird.

Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

EIN PRODUKT DER
Aagon GmbH
Lange Wende 33
D-59494 Soest
Fon: +49 (0)2921 - 789200
Fax: +49 (0)2921 - 789244
sales@aagon.com
www.aagon.com

GOLD
UNIFIED ENDPOINT MANAGEMENT
IP INSIDER
AWARD 2023

techconsult
PUR 2023
Professional User Rating
★ 4-FACH ★
★ CHAMPION ★