

Bitlocker in einer AD-Umgebung

Diese Anleitung umfasst:

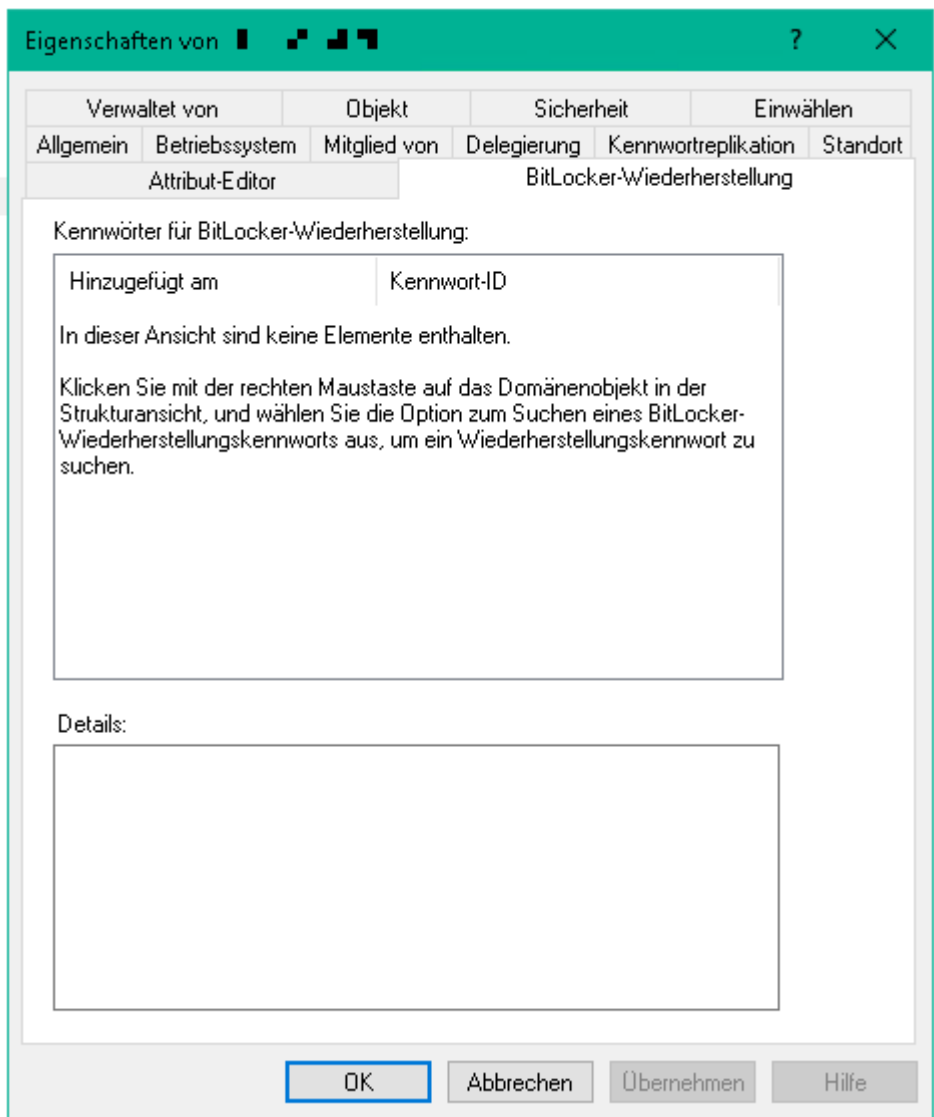
- Schlüssel in der AD gespeichert
- TPM wird vorausgesetzt
- Bitlocker wird am Rechner manuell aktiviert

Feature auf dem DC

Damit der im AD abgelegte Schlüssel in der Konsole „Active Directory Users & Computers“ nachgeschlagen werden kann, muss über den Servermanager folgendes Feature installiert werden. Dies muss auf jedem Domain Controller geschehen, über den die Schlüssel verwaltet werden sollen.



In der Konsole sollte das hinterher so aussehen:



Das Feature installiert nicht nur die Tools, sondern auch die Schemaerweiterung im AD, in der die Informationen abgelegt werden. Mittels folgenden Powershell-Befehl.

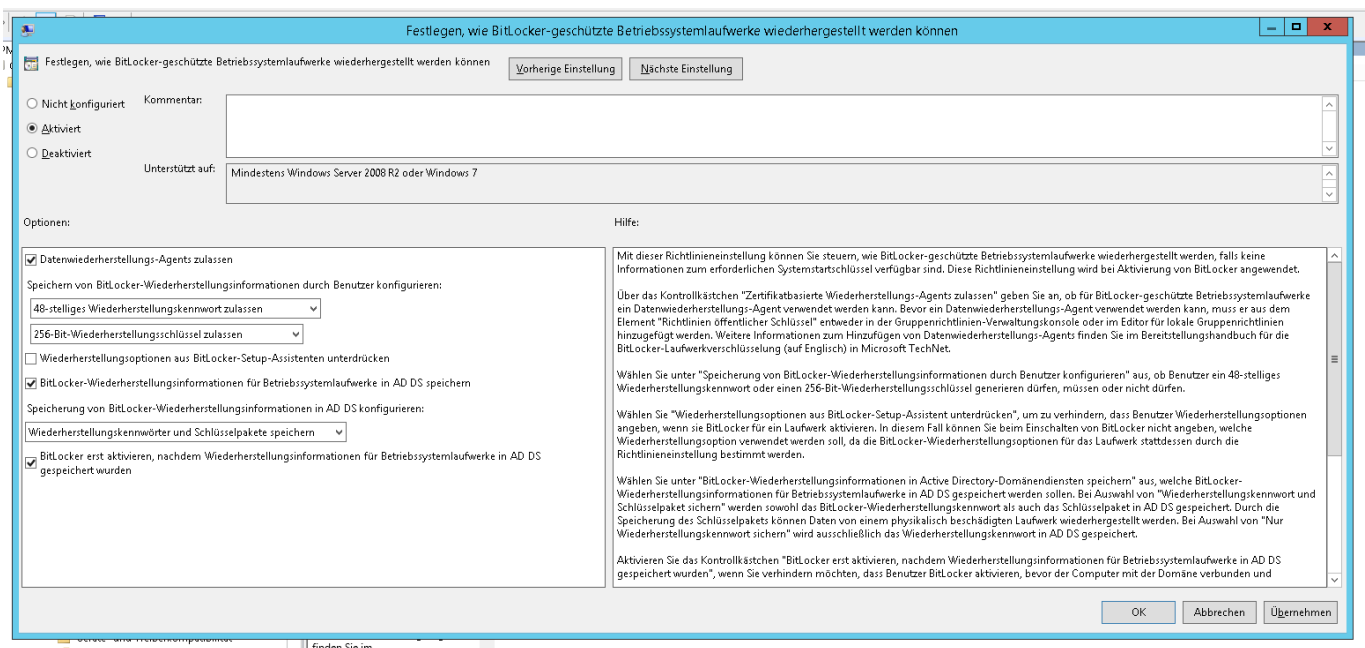
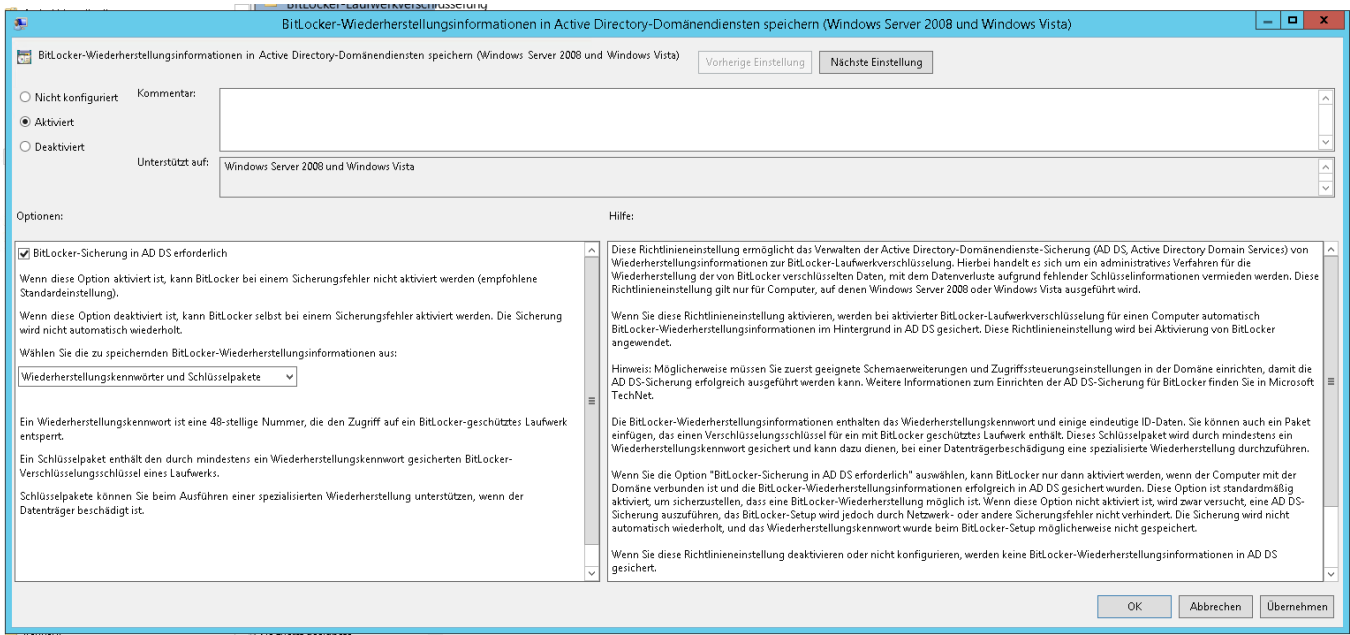
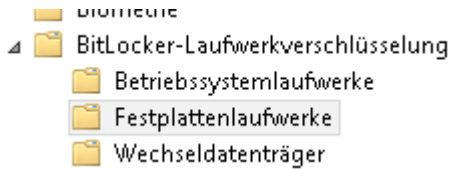
```
Get-ADObject -SearchBase ((GET-ADRootDSE).SchemaNamingContext) -Filter {Name -like 'ms-FVE-*'}
```

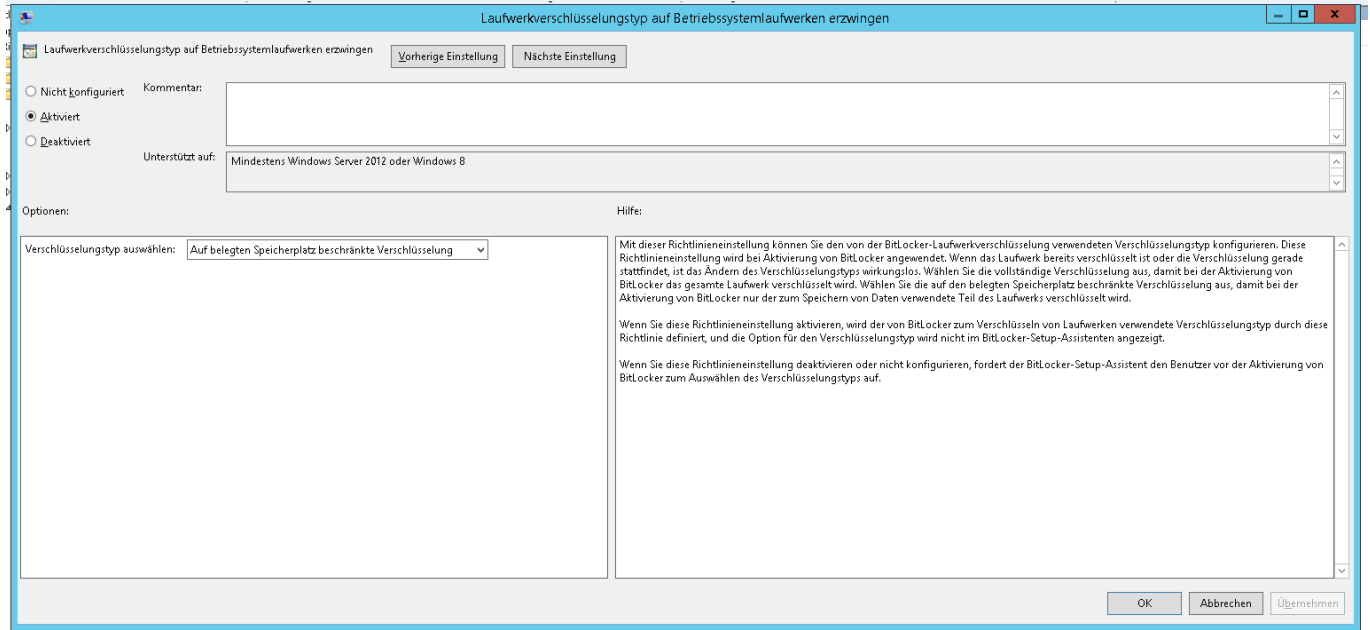
DistinguishedName ObjectGUID	Name	ObjectClass
----- -----	----- -----	----- -----
CN=ms-FVE-KeyPackage,CN=Sc... 80dd0b7b-4c78-4305-9844-ce...	ms-FVE-KeyPackage	attributeSchema
CN=ms-FVE-RecoveryGuid,CN=... d9b3a270-ce1a-4514-9f73-c2...	ms-FVE-RecoveryGuid	attributeSchema
CN=ms-FVE-RecoveryInformat... 82dac378-fa82-46ae-a49f-16...	ms-FVE-RecoveryInformation	classSchema
CN=ms-FVE-RecoveryPassword... 1b97cf96-65b7-4939-834c-ff...	ms-FVE-RecoveryPassword	attributeSchema
CN=ms-FVE-VolumeGuid,CN=Sc... 47080651-54da-4a8b-bfc9-a0...	ms-FVE-VolumeGuid	attributeSchema

Gruppenrichtlinie für die Clients

Computerkonfiguration → Richtlinien → Administrative Vorlagen → Windows-Komponenten → BitLocker-Laufwerksverschlüsselung

Die Konfiguration muss jeweils für das Betriebssystem-Laufwerk, (weitere) Festplattenlaufwerke sowie Wechseldatenträger erfolgen:





From:
<https://wiki.sebastianhetzel.net/> - **Sebastians IT-Wiki**

Permanent link:
https://wiki.sebastianhetzel.net/win_server:ad_bitlocker?rev=1633347184

Last update: **2021/10/04 13:33**

