Windows Bitlocker einsetzen

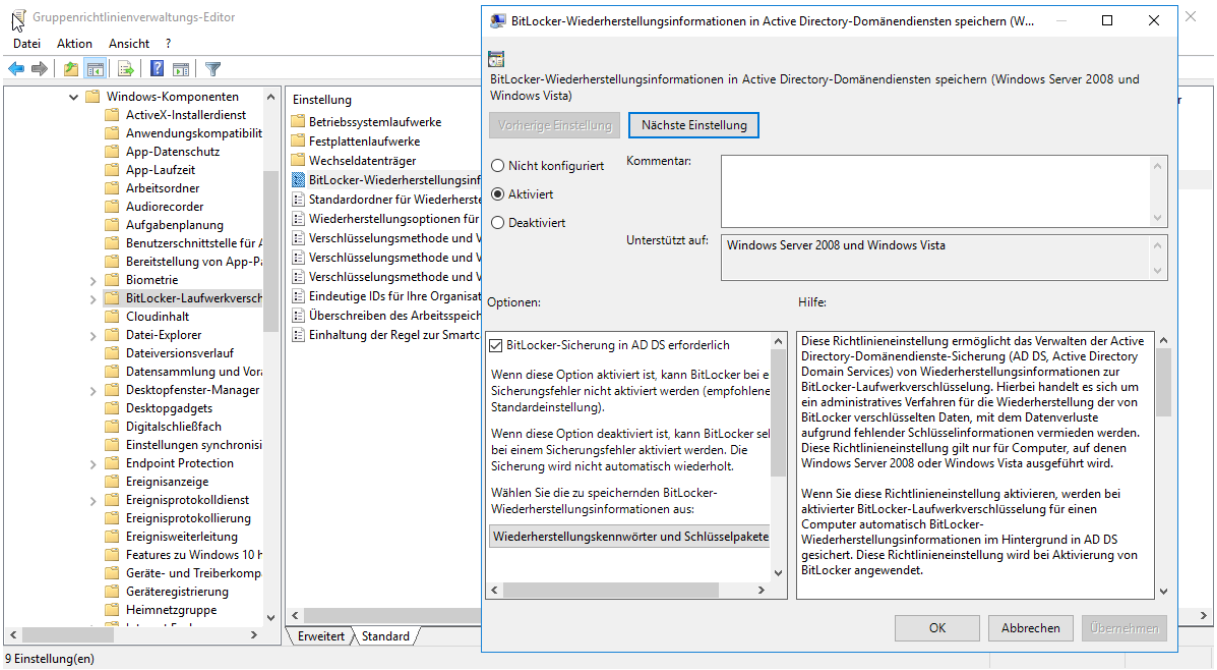
Zur Verschlüsselung der Festplatte eignet sich der Windows Bitlocker hervorragend. Alle notwendigen Einstellungen lassen sich einfach und schnell per Gruppenrichtlinie verteilen.

Folgende Einstellungen nehme ich vor, um dem User die Verschlüsselung der Festplatte zu ermöglichen. Würde ich diese erzwingen wollen, müsste ich jetzt noch MBAM installieren, dazu mehr in einer weiteren Anleitung.

Als erstes erstelle ich ein neues GPO mit dem Namen Bitlocker und konfiguriere dieses wie folgt:

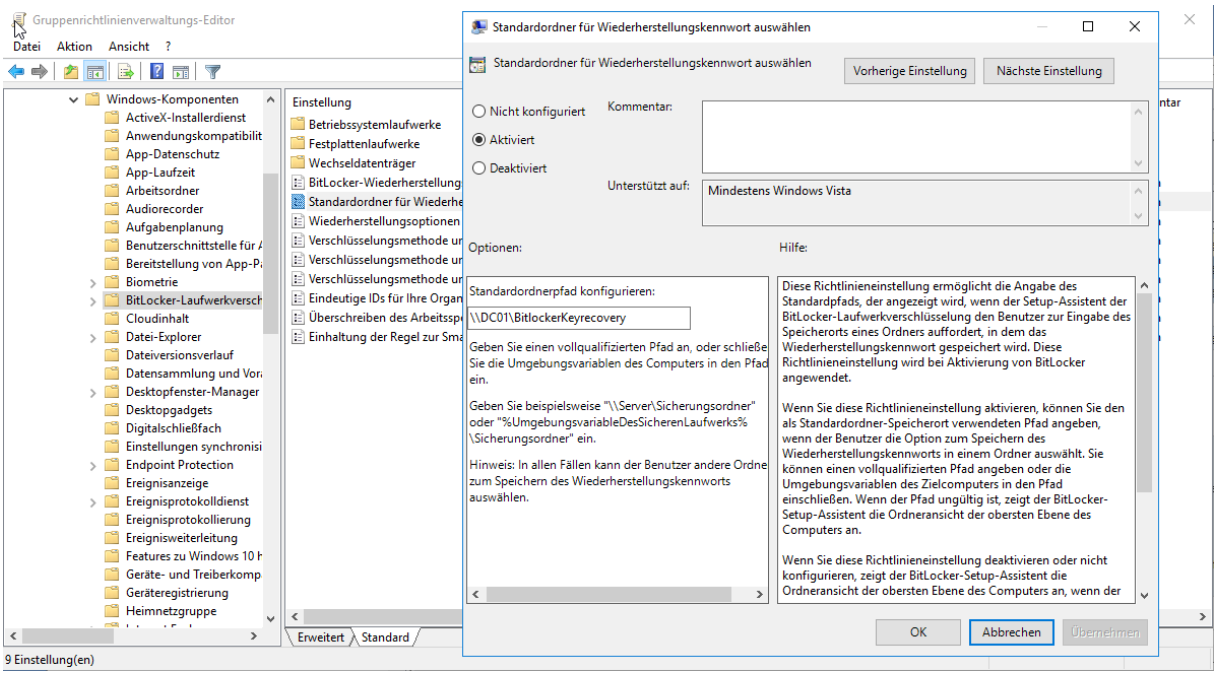
Über Computerkonfiguration > Richtlinien > Administrative Vorlagen > Windows-Komponenten > Bitlocker-Laufwerksverschlüsselung gelangen wir zu den Einstellungen.

Aktiviere die Speicherung des Wiederherstellungsschlüssels im Active Directory:

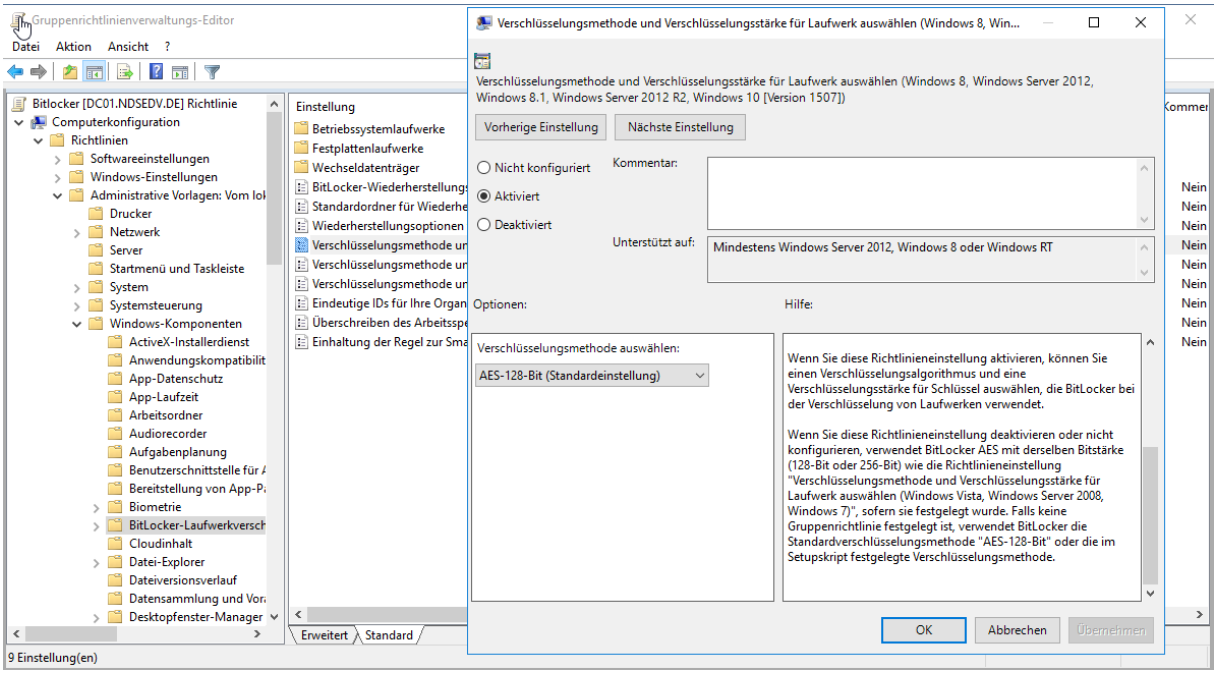


Windows Bitlocker einsetzen

Aktiviere die Speicherung des Wiederherstellungsschlüssels auf einem Netzlaufwerk:

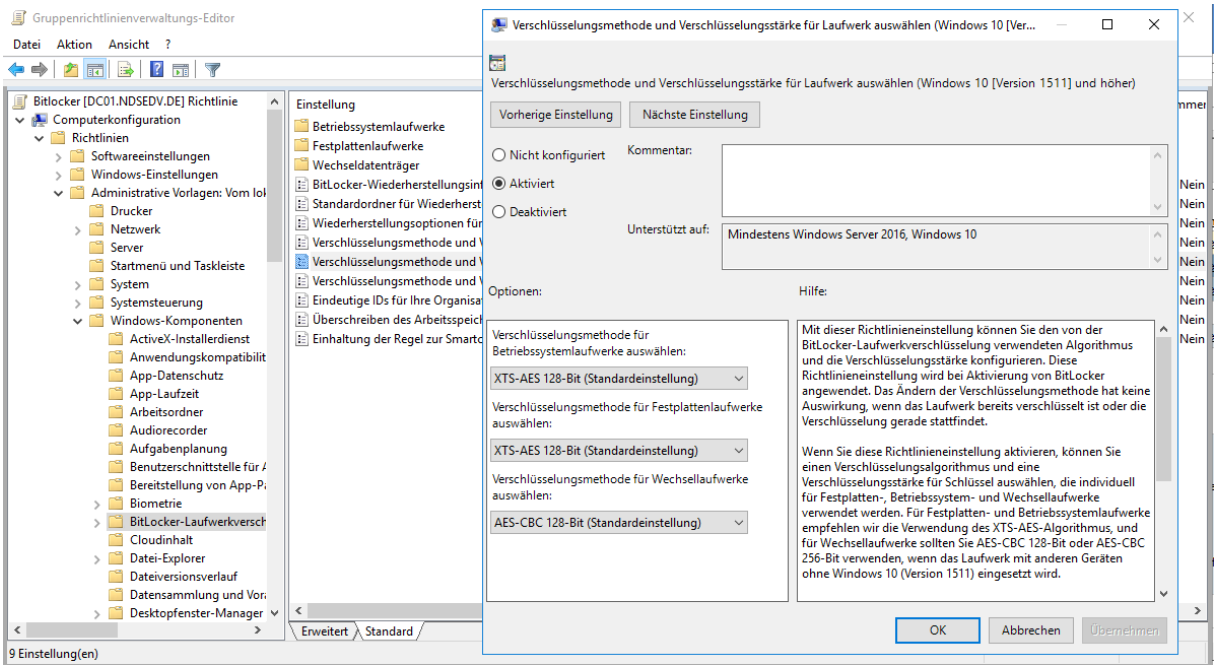


Wählen die Höhe der Verschlüsselungsstufe 128 oder 256 Bit für Systeme von Windows bis Server 2012 R2:

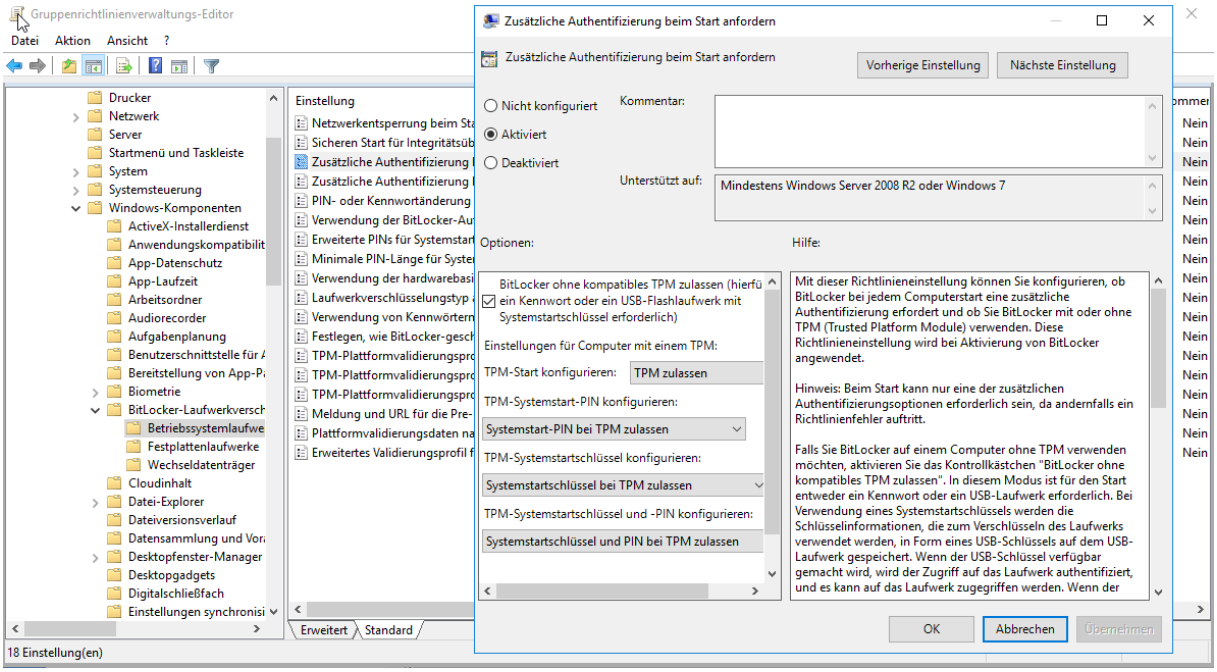


Windows Bitlocker einsetzen

Wählen die Höhe der Verschlüsselungsstufe 128 oder 256 Bit für Systeme von Windows 10 und höher, Server 2016:

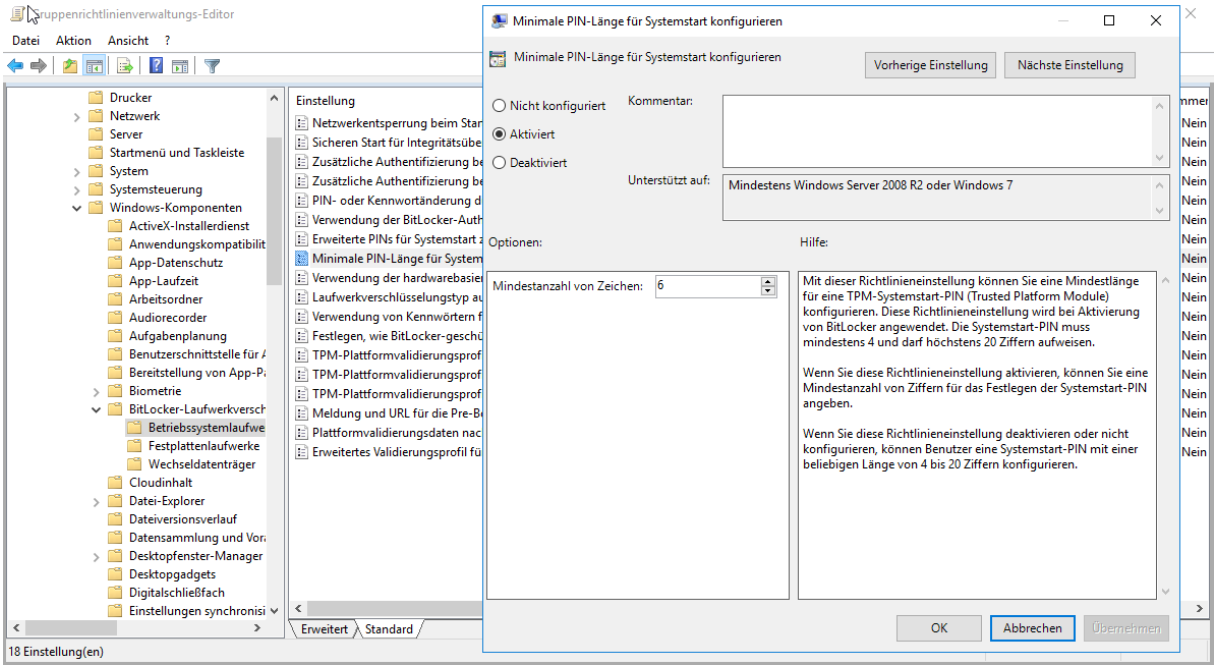


Konfigurieren nun die Kern-Optionen:

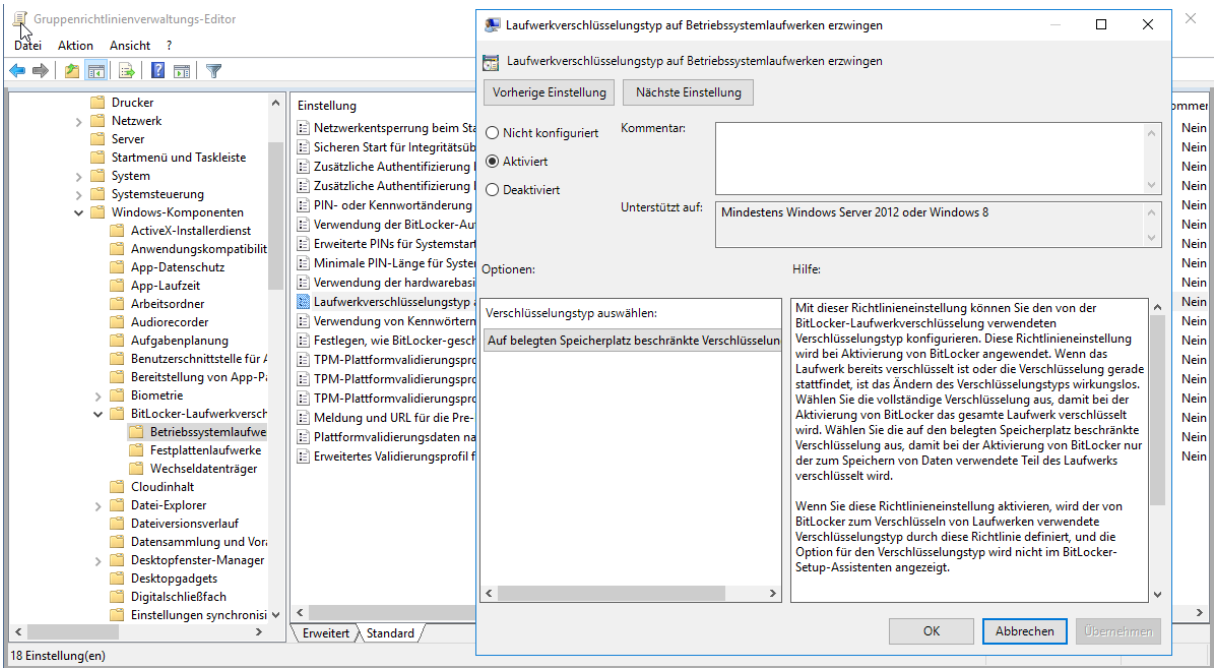


Windows Bitlocker einsetzen

Je nach gewählter Entschlüsselungs- Authentifizierungsmethode vergeben wir die PIN Mindestlänge:

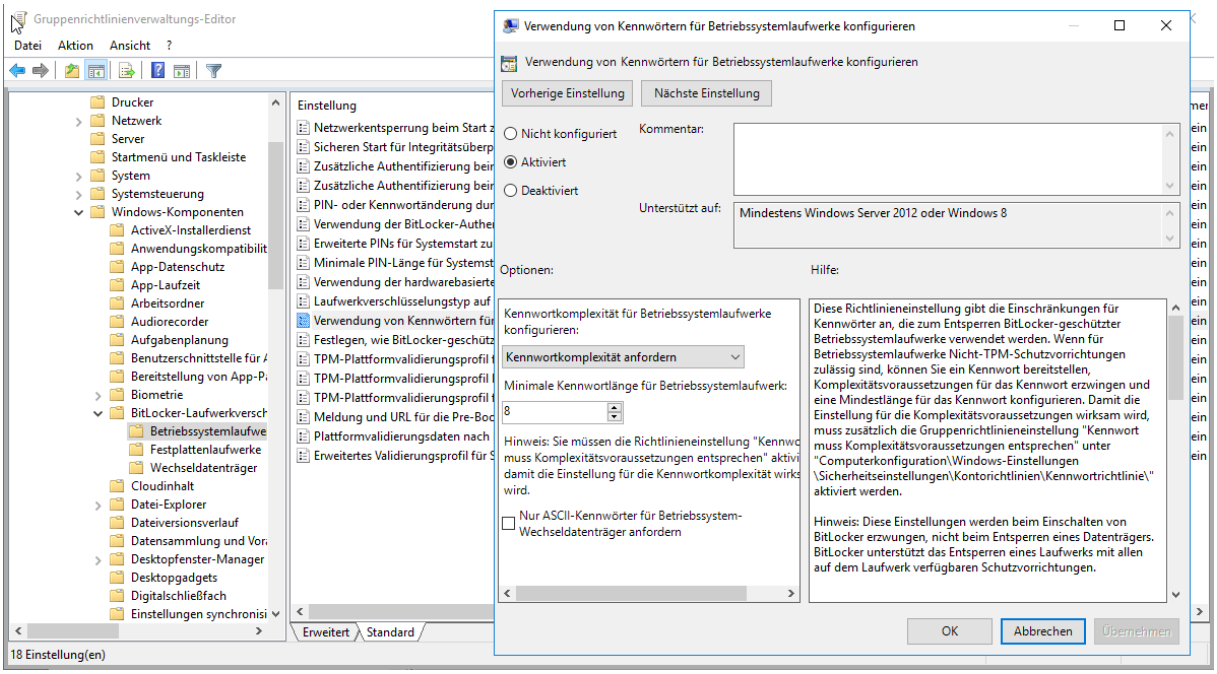


Bitlocker anweisen nur den verwendeten Speicherplatz zu verschlüsseln:

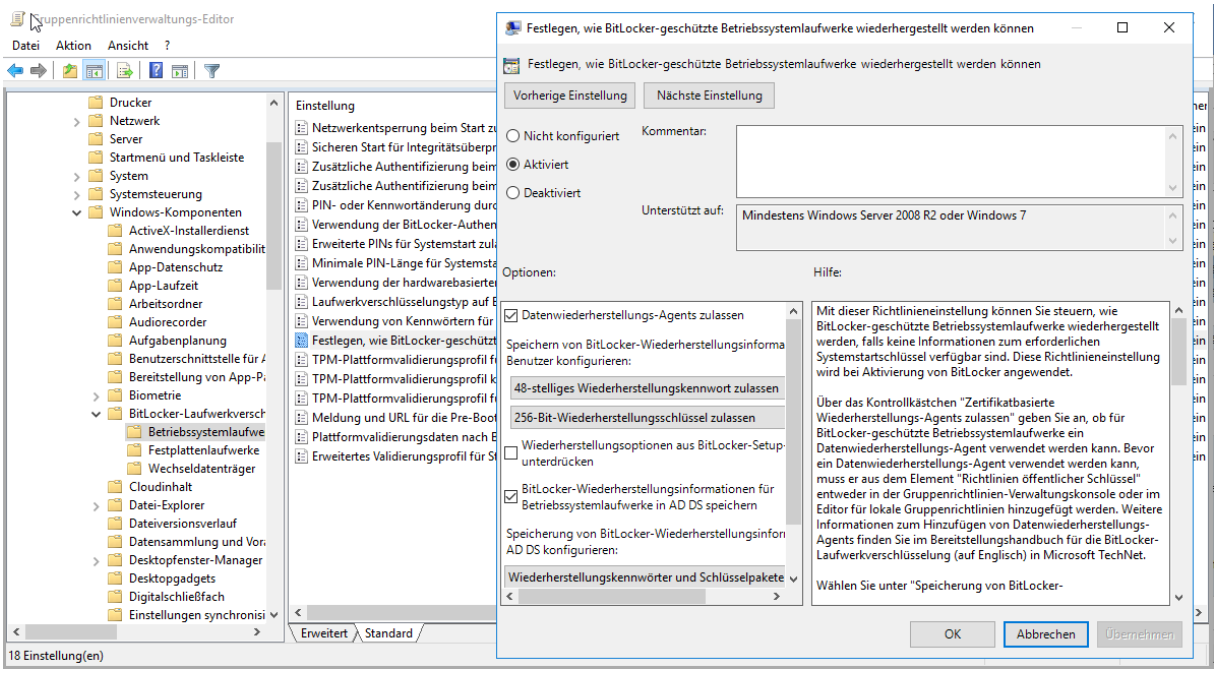


Windows Bitlocker einsetzen

Je nach gewählter Entschlüsselungs- Authentifizierungsmethode aktivieren wir auch die Verwendung von Kennwörtern:

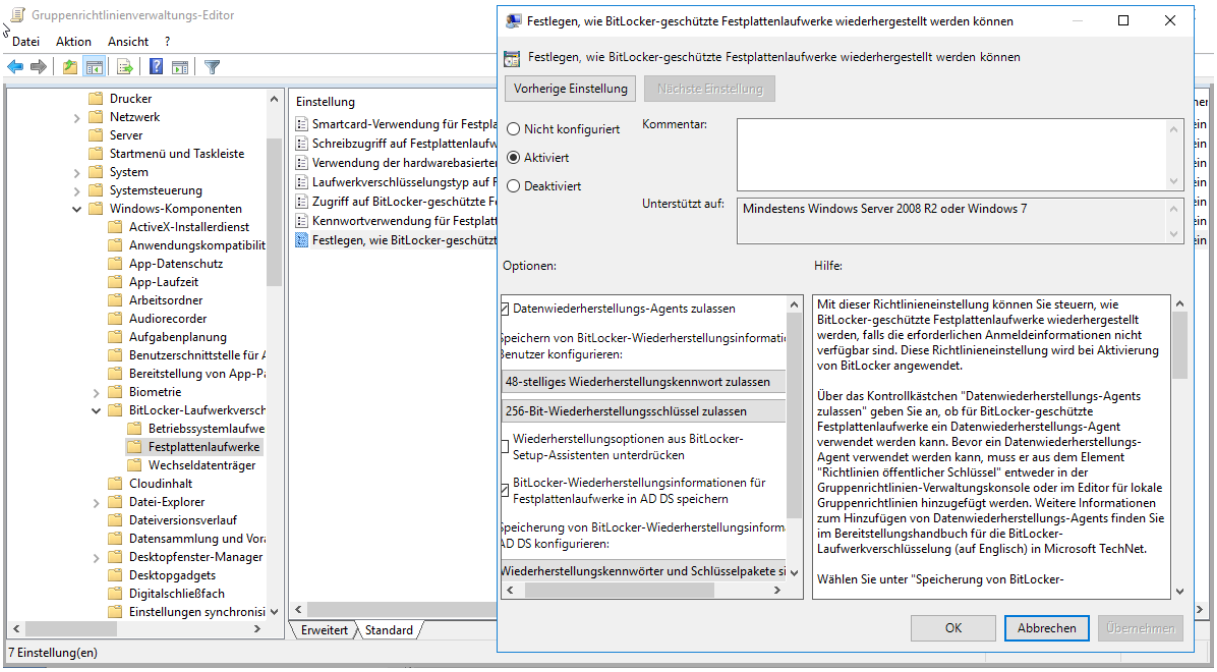


Bitlocker Wiederherstellungsmethoden für OS Platten konfigurieren:

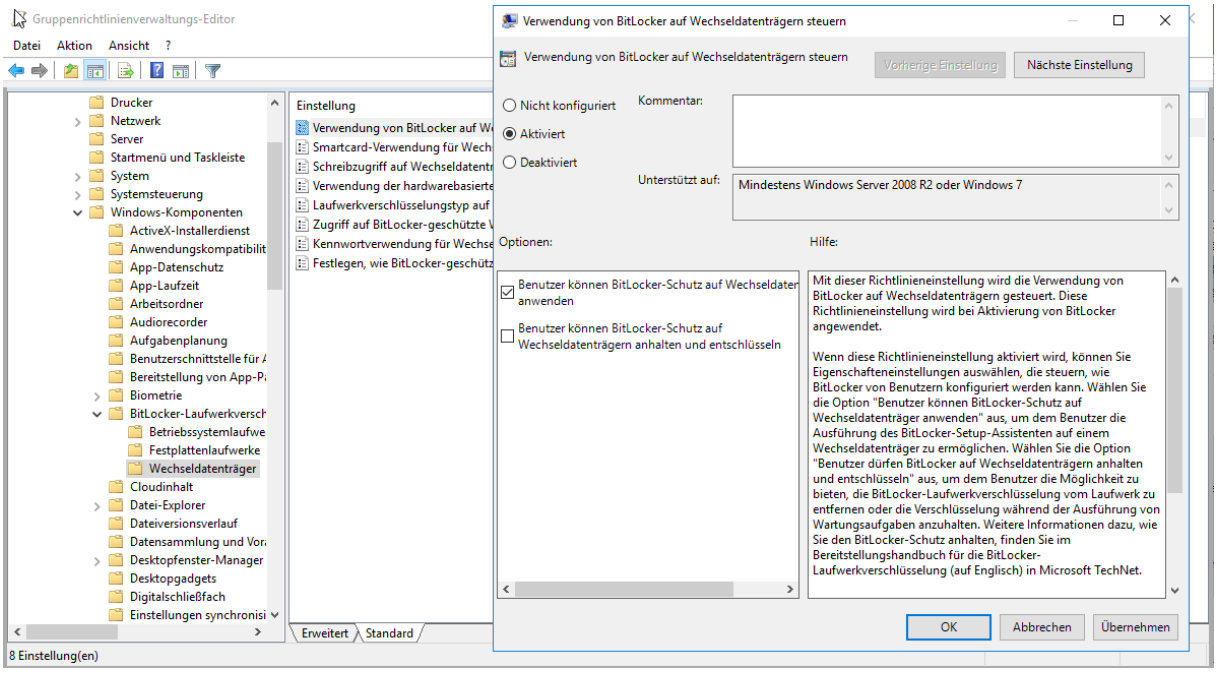


Windows Bitlocker einsetzen

Bitlocker Wiederherstellungsmethoden für weitere Platten konfigurieren:

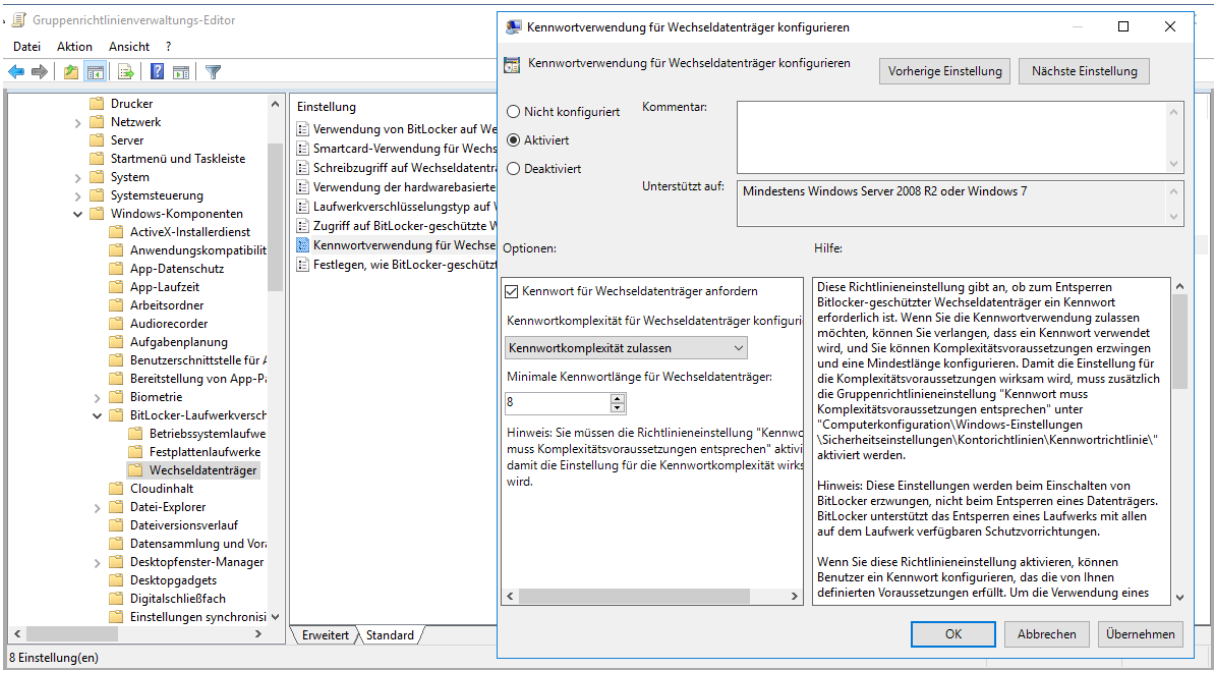


Dem User auch die Möglichkeit bieten Wechseldatenträger zu verschlüsseln:

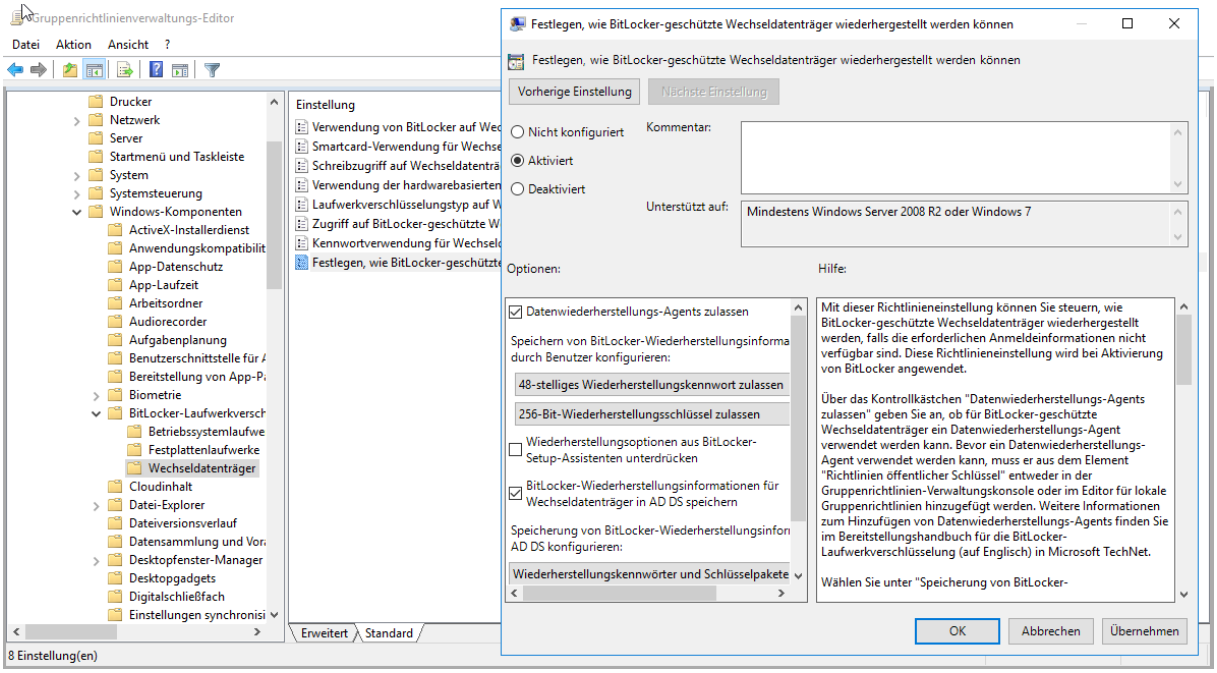


Windows Bitlocker einsetzen

Auch für Wechseldatenträger kann die Kennwort Komplexität bestimmt werden:

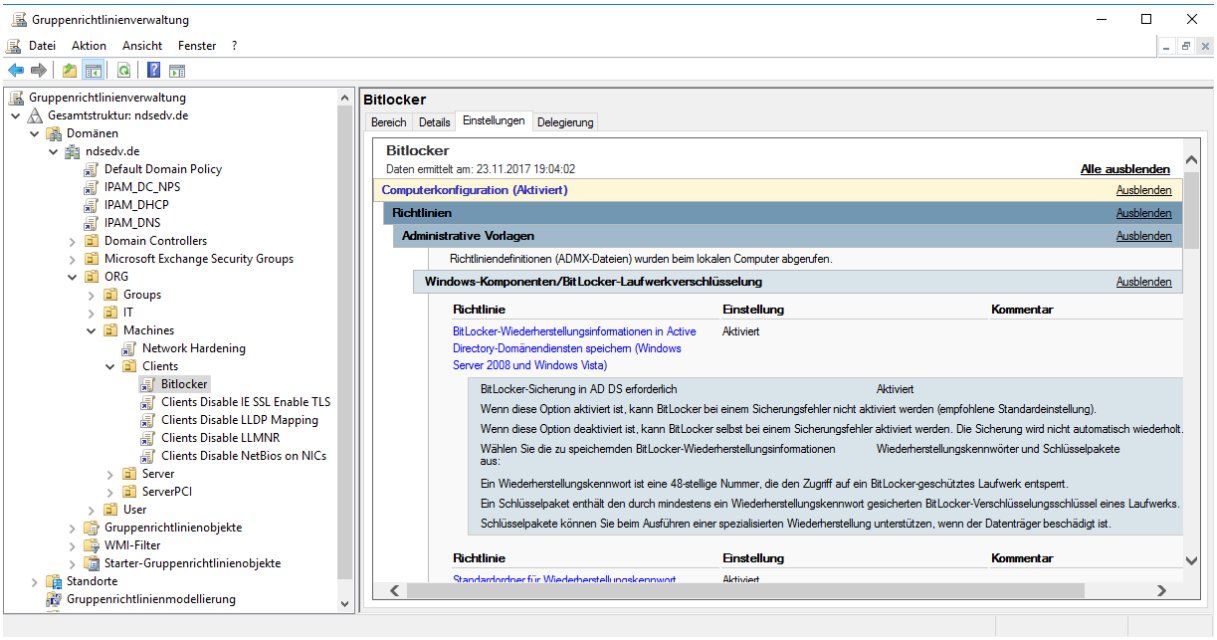


Bitlocker Wiederherstellungsmethoden konfigurieren. Bitlocker erst aktivieren, wenn die Wiederherstellungsinformationen im AD DS gespeichert wurden anhaken:

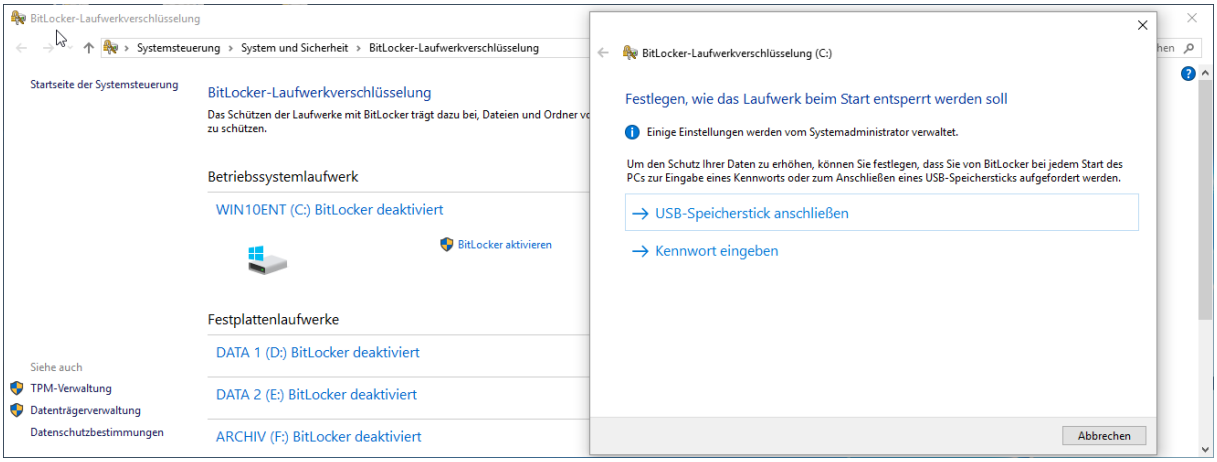


Windows Bitlocker einsetzen

Das erstellte GPO verlinken wir auf die OU in der die Clientsysteme abgelegt sind:

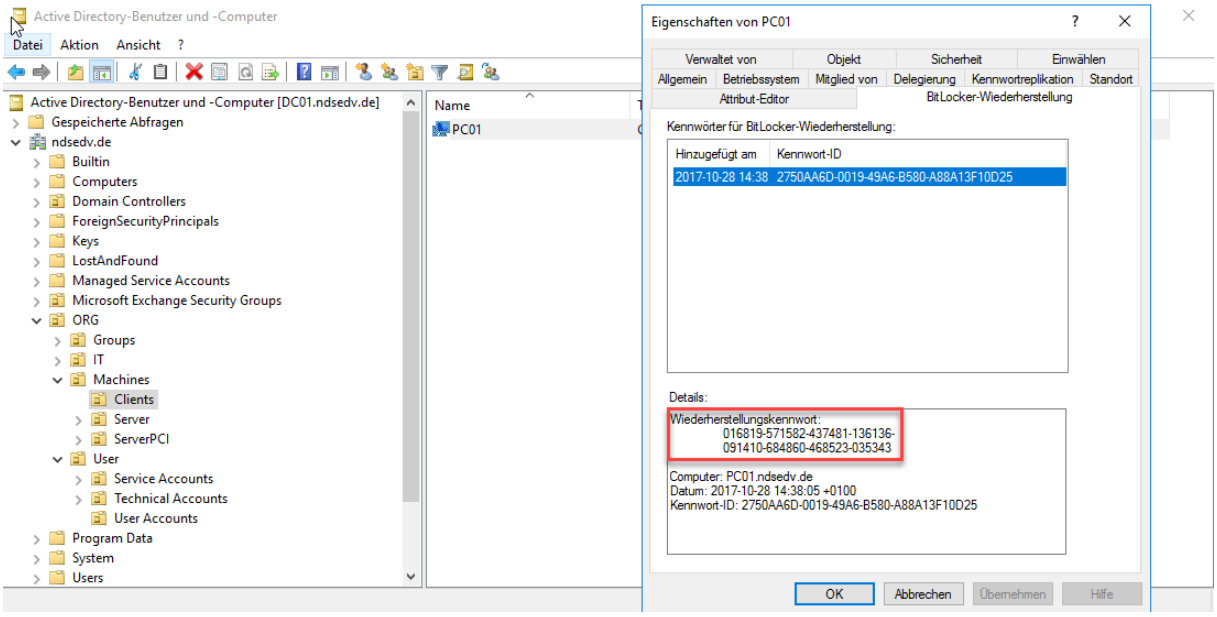


Nach einem GPUpdate /force auf dem Clientsystem und einem Neustart kann die Konfiguration Client-seitig beginnen.

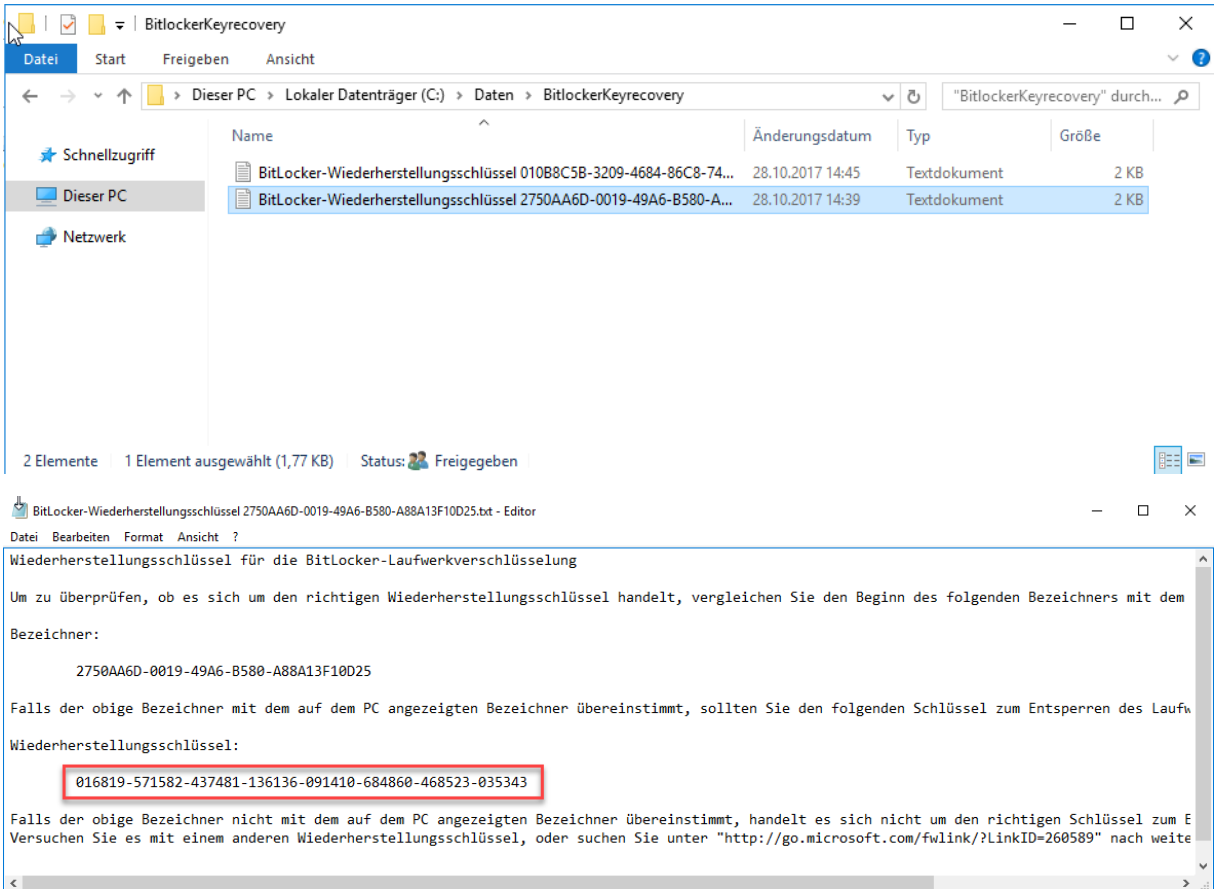


Windows Bitlocker einsetzen

Nach erfolgter Konfiguration können wir im AD DS die Wiederherstellungsschlüssel einsehen:



Als Datei abgelegt im konfiguriertem Netzlaufwerk:



Windows Bitlocker einsetzen

Powershell:

Verschlüsselung aktivieren:
manage-bde -on C:

Bitlocker aktivieren und RecoveryKey erstellen RandomKey:
manage-bde -on C: -RecoveryKey Y: -RecoveryPassword

Bitlocker deaktivieren:
manage-bde -off C:
manage-bde.exe –protectors –disable C:

Status abfragen:
manage-bde -status

Methoden abfragen:
manage-bde -protectors -get c:

Schlüssel löschen:
manage-bde -protectors -delete c: -id {xxx}

TPM aufheben:
manage-bde -protectors -delete c: -type tpm

Preboot TPM und KEY aktivieren:
manage-bde -protectors -add c: -TPMAndStartupKey x:

Preboot TPM und PIN aktivieren:
manage-bde -protectors -add c: -TPMAndPIN x:

Preboot TPM PIN und USB aktivieren:
manage-bde -protectors -add C: -TPMandPINandStartupKey -tp "Kennwort" -tsk E:

PreBootPIN deaktivieren:
manage-bde -protectors -add c: -TPM

manage-bde -status c:
Bitlocker auf C aktivieren und RecoveryKey auf D speichern:

cscript C:\Windows\System32\manage-bde.wsf -on C: -rp -sk D:
Platte C mit Passwort entsperren:

manage-bde -unlock D: -Password
Platte C mit Recovery Passwort entsperren 48 Digits:

manage-bde –unlock C: -RecoveryPassword 111111-222222-333333-444444-555555-666666-777777-888888

Platte C mit Recovery Key entsperren:
manage-bde -unlock C: -RecoveryKey "Der Pfad zur Datei Keyfile.bek"

Optional:
Recovery Password: nummerisches Kennwort
Password: benutzerdefiniertes Kennwort
RecoveryKey: *.bek komplexer Schlüssel
StartupKey: gleich wie der RecoveryKey

Erstellt von Jörn Walter **24.11.2017**

Authentication method	Requires user interaction	Description
TPM only	No	TPM validates early boot components.
TPM + PIN	Yes	TPM validates early boot components. The user must enter the correct PIN before the start-up process can continue, and before the drive can be unlocked. The TPM will enter lockout if the incorrect PIN is entered repeatedly to protect the PIN from brute force attacks. The number of repeated attempts that will trigger a lockout is variable.
TPM + Network key	No	The TPM successfully validates early boot components, and a valid encrypted network key has been provided from the WDS server. This authentication method provides automatic unlock of operating system volumes at system reboot while still maintaining multifactor authentication.
TPM + startup key	Yes	The TPM successfully validates early boot components, and a USB flash drive containing the startup key has been inserted.
Startup key only	Yes	The user is prompted to insert the USB flash drive that holds the recovery key and/or startup key and reboot the computer.

StartupKey only = RecoveryKey oder StartupKey
TPM + StartupKey = Hardware und StartupKey
TPM + PIN = Hardware und PIN
TPM only = nur Hardware
TPM + Network = Hardware + WDS Server