



## 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:

The screenshot shows the Group Policy Editor window with the following settings for the policy 'BitLocker-Wiederherstellungsinformationen in Active Directory-Domänendiensten speichern (Windows Server 2008 und Windows Vista)':

- Optionen:**
  - BitLocker-Sicherung in AD DS erforderlich
- Wählen Sie die zu speichernden BitLocker-Wiederherstellungsinformationen aus:**
  - Wiederstellungskennwörter und Schlüsselpakete

The 'Hilfe:' section contains the following text:

Diese Richtlinieneinstellung ermöglicht das Verwalten der Active Directory-Domänendienste-Sicherung (AD DS, Active Directory Domain Services) von Wiederherstellungsinformationen zur BitLocker-Laufwerksverschlüsselung. Hierbei handelt es sich um ein administratives Verfahren für die Wiederherstellung der von BitLocker verschlüsselten Daten, mit dem Datenverluste aufgrund fehlender Schlüsselinformationen vermieden werden. Diese Richtlinieneinstellung gilt nur für Computer, auf denen Windows Server 2008 oder Windows Vista ausgeführt wird.

Wenn Sie diese Richtlinieneinstellung aktivieren, werden bei aktivierter BitLocker-Laufwerksverschlüsselung für einen Computer automatisch BitLocker-Wiederherstellungsinformationen im Hintergrund in AD DS gesichert. Diese Richtlinieneinstellung wird bei Aktivierung von BitLocker angewendet.



## Windows BitLocker einsetzen

Aktiviere die Speicherung des Wiederherstellungsschlüssels auf einem Netzlaufwerk:

The screenshot shows the Group Policy Editor (Gruppenrichtlinienverwaltungs-Editor) with the following settings:

- Standardordner für Wiederherstellungskennwort auswählen**:
  - Aktiviert
  - Unterstützt auf: Mindestens Windows Vista
  - Standardordnerpfad konfigurieren: \\DC01\BitLockerKeyrecovery

The help text explains that this setting allows specifying a standard path for the recovery key. It notes that when activated, the BitLocker Setup Assistant will prompt for a folder path to store the key. The help also mentions that users can specify a fully qualified path or use environment variables like %Server\Sicherungsordner% or %UmgebungsvariableDesSicherenLaufwerks%\Sicherungsordner%.

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

The screenshot shows the Group Policy Editor (Gruppenrichtlinienverwaltungs-Editor) with the following settings:

- Verschlüsselungsmethode und Verschlüsselungsstärke für Laufwerk auswählen (Windows 8, Win...)**:
  - Aktiviert
  - Unterstützt auf: Mindestens Windows Server 2012, Windows 8 oder Windows RT
  - Verschlüsselungsmethode auswählen: AES-128-Bit (Standardeinstellung)

The help text states that when this setting is activated, users can choose an encryption algorithm and a key strength (128-bit or 256-bit) for the encryption of drives. It also notes that if the setting is deactivated, BitLocker will use AES with the same key strength (128-bit or 256-bit) as the policy setting for the encryption of drives.



## Windows Bitlocker einsetzen

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

Gruppenrichtlinienverwaltungs-Editor

Verschlüsselungsmethode und Verschlüsselungsstärke für Laufwerk auswählen (Windows 10 [Ver...])

Verschlüsselungsmethode und Verschlüsselungsstärke für Laufwerk auswählen (Windows 10 [Version 1511] und höher)

Vorherige Einstellung Nächste Einstellung

Nicht konfiguriert Kommentar:

Aktiviert

Deaktiviert

Unterstützt auf: Mindestens Windows Server 2016, Windows 10

Optionen:

Verschlüsselungsmethode für Betriebssystemlaufwerke auswählen: XTS-AES 128-Bit (Standardeinstellung)

Verschlüsselungsmethode für Festplattenlaufwerke auswählen: XTS-AES 128-Bit (Standardeinstellung)

Verschlüsselungsmethode für Wechsellaufwerke auswählen: AES-CBC 128-Bit (Standardeinstellung)

Hilfe:

Mit dieser Richtlinieneinstellung können Sie den von der BitLocker-Laufwerkverschlüsselung verwendeten Algorithmus und die Verschlüsselungsstärke konfigurieren. Diese Richtlinieneinstellung wird bei Aktivierung von BitLocker angewendet. Das Ändern der Verschlüsselungsmethode hat keine Auswirkung, wenn das Laufwerk bereits verschlüsselt ist oder die Verschlüsselung gerade stattfindet.

Wenn Sie diese Richtlinieneinstellung aktivieren, können Sie einen Verschlüsselungsalgorithmus und eine Verschlüsselungsstärke für Schlüssel auswählen, die individuell für Festplatten-, Betriebssystem- und Wechsellaufwerke verwendet werden. Für Festplatten- und Betriebssystemlaufwerke empfehlen wir die Verwendung des XTS-AES-Algorithmus, und für Wechsellaufwerke sollten Sie AES-CBC 128-Bit oder AES-CBC 256-Bit verwenden, wenn das Laufwerk mit anderen Geräten ohne Windows 10 (Version 1511) eingesetzt wird.

OK Abbrechen Übernehmen

Konfigurieren nun die Kern-Optionen:

Gruppenrichtlinienverwaltungs-Editor

Zusätzliche Authentifizierung beim Start anfordern

Zusätzliche Authentifizierung beim Start anfordern

Vorherige Einstellung Nächste Einstellung

Nicht konfiguriert Kommentar:

Aktiviert

Deaktiviert

Unterstützt auf: Mindestens Windows Server 2008 R2 oder Windows 7

Optionen:

BitLocker ohne kompatibles TPM zulassen (hierfür ein Kennwort oder ein USB-Flashlaufwerk mit Systemstartschlüssel erforderlich)

Einstellungen für Computer mit einem TPM:

TPM-Start konfigurieren: TPM zulassen

TPM-Systemstart-PIN konfigurieren: Systemstart-PIN bei TPM zulassen

TPM-Systemstartschlüssel konfigurieren: Systemstartschlüssel bei TPM zulassen

TPM-Systemstartschlüssel und -PIN konfigurieren: Systemstartschlüssel und PIN bei TPM zulassen

Hilfe:

Mit dieser Richtlinieneinstellung können Sie konfigurieren, ob BitLocker bei jedem Computerstart eine zusätzliche Authentifizierung erfordert und ob Sie BitLocker mit oder ohne TPM (Trusted Platform Module) verwenden. Diese Richtlinieneinstellung wird bei Aktivierung von BitLocker angewendet.

Hinweis: Beim Start kann nur eine der zusätzlichen Authentifizierungsoptionen erforderlich sein, da andernfalls ein Richtlinienfehler auftritt.

Falls Sie BitLocker auf einem Computer ohne TPM verwenden möchten, aktivieren Sie das Kontrollkästchen "BitLocker ohne kompatibles TPM zulassen". In diesem Modus ist für den Start entweder ein Kennwort oder ein USB-Laufwerk erforderlich. Bei Verwendung eines Systemstartschlüssels werden die Schlüsselinformationen, die zum Verschlüsseln des Laufwerks verwendet werden, in Form eines USB-Schlüssels auf dem USB-Laufwerk gespeichert. Wenn der USB-Schlüssel verfügbar gemacht wird, wird der Zugriff auf das Laufwerk authentifiziert, und es kann auf das Laufwerk zugegriffen werden. Wenn der

OK Abbrechen Übernehmen



## Windows Bitlocker einsetzen

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

The screenshot shows the Group Policy Editor window with the following details:

- Policy Name:** Minimale PIN-Länge für Systemstart konfigurieren
- Configuration:**  Aktiviert
- Comment:** (Empty)
- Supported on:** Mindestens Windows Server 2008 R2 oder Windows 7
- Options:** Mindestanzahl von Zeichen: 6
- Help:** Mit dieser Richtlinieneinstellung können Sie eine Mindestlänge für eine TPM-Systemstart-PIN (Trusted Platform Module) konfigurieren. Diese Richtlinieneinstellung wird bei Aktivierung von BitLocker angewendet. Die Systemstart-PIN muss mindestens 4 und darf höchstens 20 Ziffern aufweisen. Wenn Sie diese Richtlinieneinstellung aktivieren, können Sie eine Mindestanzahl von Ziffern für das Festlegen der Systemstart-PIN angeben. Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, können Benutzer eine Systemstart-PIN mit einer beliebigen Länge von 4 bis 20 Ziffern konfigurieren.

Bitlocker anweisen nur den verwendeten Speicherplatz zu verschlüsseln:

The screenshot shows the Group Policy Editor window with the following details:

- Policy Name:** Laufwerkverschlüsselungstyp auf Betriebssystemlaufwerken erzwingen
- Configuration:**  Aktiviert
- Comment:** (Empty)
- Supported on:** Mindestens Windows Server 2012 oder Windows 8
- Options:** Verschlüsselungstyp auswählen: Auf belegten Speicherplatz beschränkte Verschlüsselung
- Help:** Mit dieser Richtlinieneinstellung können Sie den von der BitLocker-Laufwerkverschlüsselung verwendeten Verschlüsselungstyp konfigurieren. Diese Richtlinieneinstellung wird bei Aktivierung von BitLocker angewendet. Wenn das Laufwerk bereits verschlüsselt ist oder die Verschlüsselung gerade stattfindet, ist das Ändern des Verschlüsselungstyps wirkungslos. Wählen Sie die vollständige Verschlüsselung aus, damit bei der Aktivierung von BitLocker das gesamte Laufwerk verschlüsselt wird. Wählen Sie die auf den belegten Speicherplatz beschränkte Verschlüsselung aus, damit bei der Aktivierung von BitLocker nur der zum Speichern von Daten verwendete Teil des Laufwerks verschlüsselt wird. Wenn Sie diese Richtlinieneinstellung aktivieren, wird der von BitLocker zum Verschlüsseln von Laufwerken verwendete Verschlüsselungstyp durch diese Richtlinie definiert, und die Option für den Verschlüsselungstyp wird nicht im BitLocker-Setup-Assistenten angezeigt.



## Windows BitLocker einsetzen

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

The screenshot shows the Group Policy Editor window with the following settings:

- Verwendung von Kennwörtern für Betriebssystemlaufwerke konfigurieren:**
  - Aktiviert
  - Unterstützt auf: Mindestens Windows Server 2012 oder Windows 8
  - Optionen:
    - Kennwortkomplexität für Betriebssystemlaufwerke konfigurieren: **Kennwortkomplexität anfordern**
    - Minimale Kennwortlänge für Betriebssystemlaufwerk: **8**
  - Hinweis: Sie müssen die Richtlinieneinstellung "Kennwort muss Komplexitätsvoraussetzungen entsprechen" aktivieren, damit die Einstellung für die Kennwortkomplexität wirksam wird.
  - Nur ASCII-Kennwörter für Betriebssystem-Wechseldatenträger anfordern
- Hilfe:**

Diese Richtlinieneinstellung gibt die Einschränkungen für Kennwörter an, die zum Entsperren BitLocker-geschützter Betriebssystemlaufwerke verwendet werden. Wenn für Betriebssystemlaufwerke Nicht-TPM-Schutzvorrichtungen zulässig sind, können Sie ein Kennwort bereitstellen, Komplexitätsvoraussetzungen für das Kennwort erzwingen und eine Mindestlänge für das Kennwort konfigurieren. Damit die Einstellung für die Komplexitätsvoraussetzungen wirksam wird, muss zusätzlich die Gruppenrichtlinieneinstellung "Kennwort muss Komplexitätsvoraussetzungen entsprechen" unter "Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Kontorichtlinien\Kennwortrichtlinie" aktiviert werden.

Hinweis: Diese Einstellungen werden beim Einschalten von BitLocker erzwingen, nicht beim Entsperren eines Datenträgers. BitLocker unterstützt das Entsperren eines Laufwerks mit allen auf dem Laufwerk verfügbaren Schutzvorrichtungen.

BitLocker Wiederherstellungsmethoden für OS Platten konfigurieren:

The screenshot shows the Group Policy Editor window with the following settings:

- Festlegen, wie BitLocker-geschützte Betriebssystemlaufwerke wiederhergestellt werden können:**
  - Aktiviert
  - Unterstützt auf: Mindestens Windows Server 2008 R2 oder Windows 7
  - Optionen:
    - Datenwiederherstellungs-Agents zulassen
    - 48-stelliges Wiederherstellungskennwort zulassen
    - 256-Bit-Wiederherstellungsschlüssel zulassen
    - Wiederherstellungsoptionen aus BitLocker-Setup unterdrücken
    - BitLocker-Wiederherstellungsinformationen für Betriebssystemlaufwerke in AD DS speichern
  - Hilfe:**

Mit dieser Richtlinieneinstellung können Sie steuern, wie BitLocker-geschützte Betriebssystemlaufwerke wiederhergestellt werden, falls keine Informationen zum erforderlichen Systemstartschlüssel verfügbar sind. Diese Richtlinieneinstellung wird bei Aktivierung von BitLocker angewendet.

Über das Kontrollkästchen "Zertifikatbasierte Wiederherstellungs-Agents zulassen" geben Sie an, ob für BitLocker-geschützte Betriebssystemlaufwerke ein Datenwiederherstellungs-Agent verwendet werden kann. Bevor ein Datenwiederherstellungs-Agent verwendet werden kann, muss er aus dem Element "Richtlinien öffentlicher Schlüssel" entweder in der Gruppenrichtlinien-Verwaltungskontrolle oder im Editor für lokale Gruppenrichtlinien hinzugefügt werden. Weitere Informationen zum Hinzufügen von Datenwiederherstellungs-Agents finden Sie im Bereitstellungshandbuch für die BitLocker-Laufwerkverschlüsselung (auf Englisch) in Microsoft TechNet.

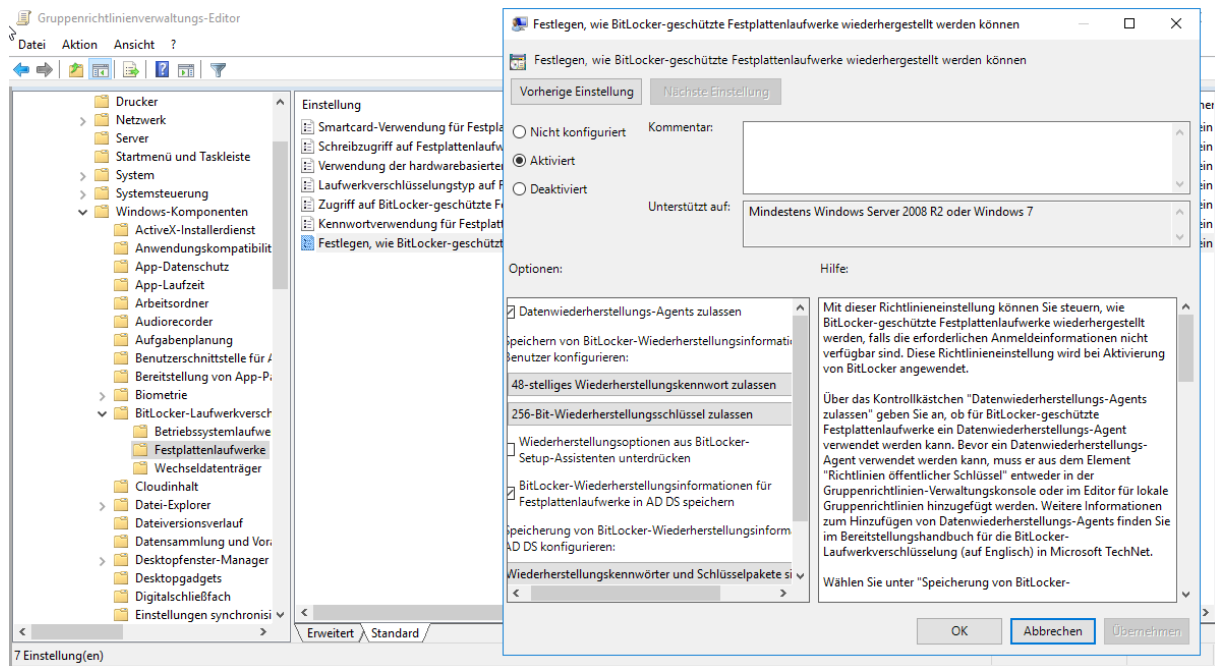
Wählen Sie unter "Speicherung von BitLocker-



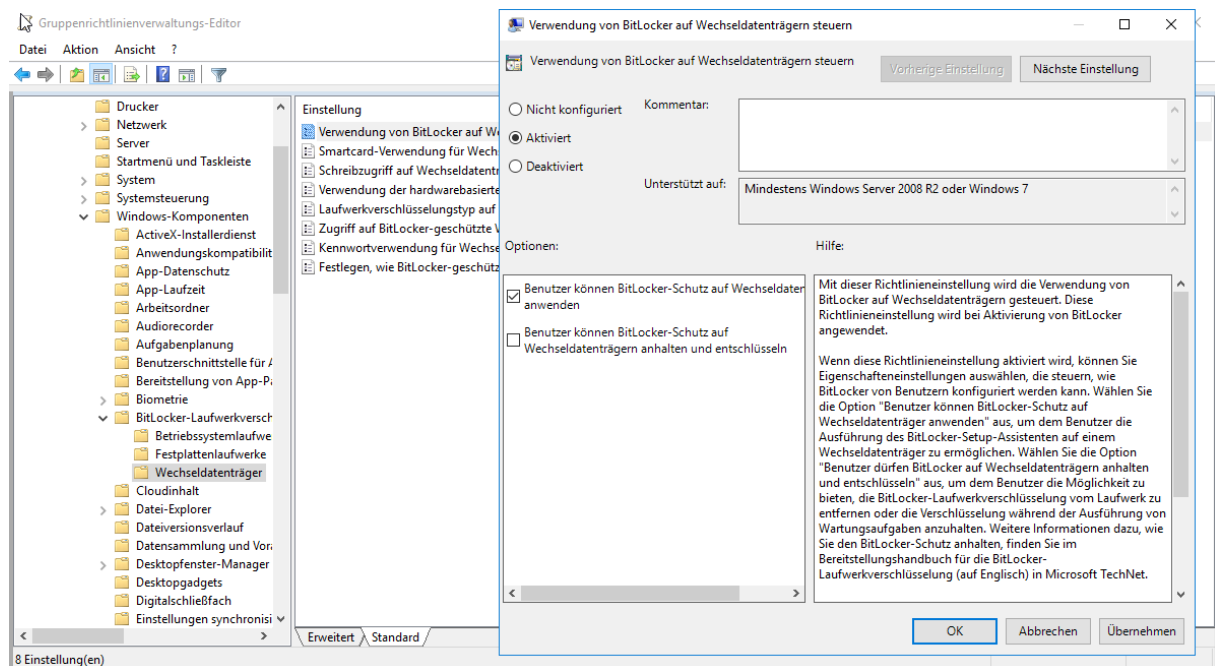


## Windows BitLocker einsetzen

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:

The screenshot shows the Group Policy Editor window with the following settings for "Kennwortverwendung für Wechseldatenträger konfigurieren":

- Aktiviert
- Unterstützt auf: Mindestens Windows Server 2008 R2 oder Windows 7
- Optionen:
  - Kennwort für Wechseldatenträger anfordern
  - Kennwortkomplexität für Wechseldatenträger konfigurieren:
  - Minimale Kennwortlänge für Wechseldatenträger:

The help text states: "Diese Richtlinieneinstellung gibt an, ob zum Entsperren BitLocker-geschützter Wechseldatenträger ein Kennwort erforderlich ist. Wenn Sie die Kennwortverwendung zulassen möchten, können Sie verlangen, dass ein Kennwort verwendet wird, und Sie können Komplexitätsvoraussetzungen erzwingen und eine Mindestlänge konfigurieren. Damit die Einstellung für die Komplexitätsvoraussetzungen wirksam wird, muss zusätzlich die Gruppenrichtlinieneinstellung 'Kennwort muss Komplexitätsvoraussetzungen entsprechen' unter 'Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Kontorichtlinien\Kennwortrichtlinie' aktiviert werden."

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

The screenshot shows the Group Policy Editor window with the following settings for "Festlegen, wie BitLocker-geschützte Wechseldatenträger wiederhergestellt werden können":

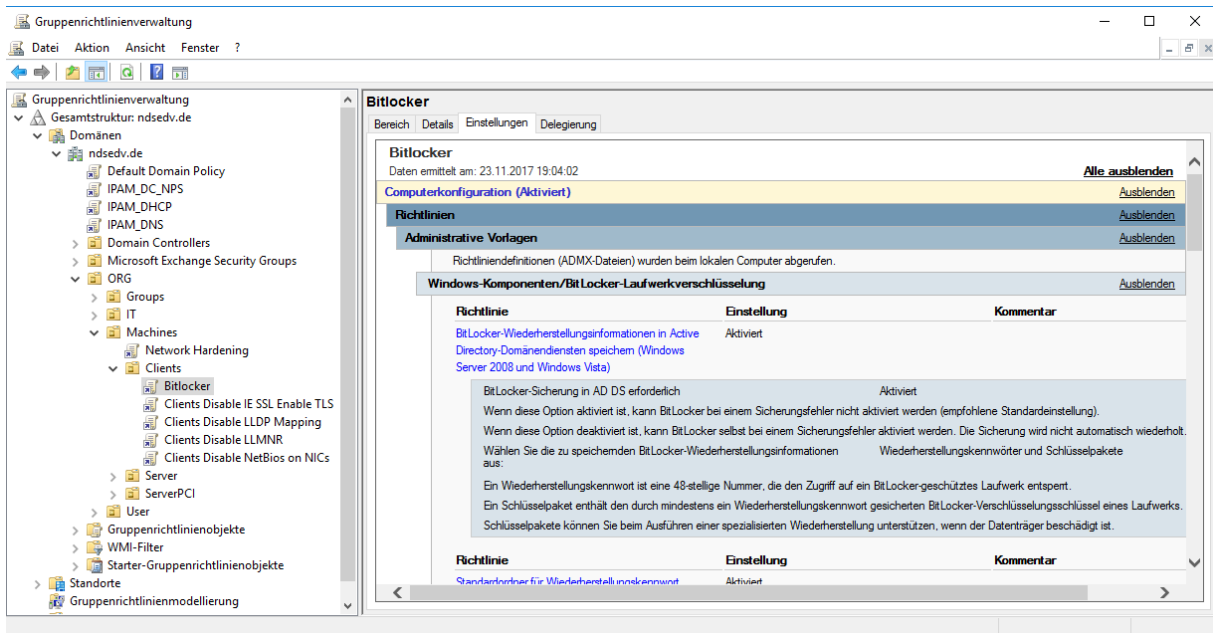
- Aktiviert
- Unterstützt auf: Mindestens Windows Server 2008 R2 oder Windows 7
- Optionen:
  - Datenwiederstellungs-Agents zulassen
  - Speichern von BitLocker-Wiederherstellungsinformationen durch Benutzer konfigurieren:
    - 48-stelliges Wiederherstellungskennwort zulassen
    - 256-Bit-Wiederherstellungsschlüssel zulassen
  - Wiederherstellungsoptionen aus BitLocker-Setup-Assistenten unterdrücken
  - BitLocker-Wiederherstellungsinformationen für Wechseldatenträger in AD DS speichern
  - Speicherung von BitLocker-Wiederherstellungsinformationen in AD DS konfigurieren:
    -

The help text states: "Mit dieser Richtlinieneinstellung können Sie steuern, wie BitLocker-geschützte Wechseldatenträger wiederhergestellt werden, falls die erforderlichen Anmeldeinformationen nicht verfügbar sind. Diese Richtlinieneinstellung wird bei Aktivierung von BitLocker angewendet."

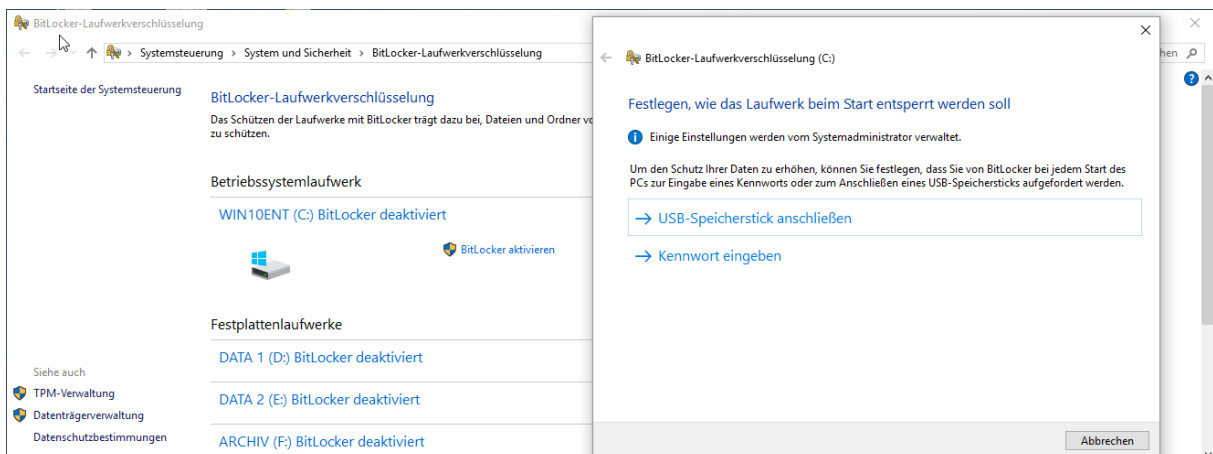


## Windows Bitlocker einsetzen

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



Nach einem GPOupdate /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:

The screenshot shows the Active Directory console with the 'Eigenschaften von PC01' (Properties of PC01) dialog box open. The 'BitLocker-Wiederherstellung' tab is selected, displaying a table of recovery keys. The 'Wiederherstellungskennwort' (Recovery key) field is highlighted with a red box.

Hinzugefügt am	Kennwort-ID
2017-10-28 14:38	2750AA6D-0019-49A6-B580-A88A13F10D25

Details:

Wiederherstellungskennwort:  
016819-571582-437481-136136-091410-684860-468523-035343

Computer: PC01.ndsedv.de  
Datum: 2017-10-28 14:38:05 +0100  
Kennwort-ID: 2750AA6D-0019-49A6-B580-A88A13F10D25

Als Datei abgelegt im konfiguriertem Netzlaufwerk:

The screenshot shows a Windows Explorer window displaying a folder named 'BitLockerKeyrecovery'. Two files are listed:

Name	Änderungsdatum	Typ	Größe
BitLocker-Wiederherstellungsschlüssel 010B8C5B-3209-4684-86C8-74...	28.10.2017 14:45	Textdokument	2 KB
BitLocker-Wiederherstellungsschlüssel 2750AA6D-0019-49A6-B580-A...	28.10.2017 14:39	Textdokument	2 KB

The second file is selected. Below it, a text editor window shows the content of the file:

Wiederherstellungsschlüssel für die BitLocker-Laufwerkverschlüsselung

Um zu überprüfen, ob es sich um den richtigen Wiederherstellungsschlüssel handelt, vergleichen Sie den Beginn des folgenden Bezeichners mit dem Bezeichner:

2750AA6D-0019-49A6-B580-A88A13F10D25

Falls der obige Bezeichner mit dem auf dem PC angezeigten Bezeichner übereinstimmt, sollten Sie den folgenden Schlüssel zum Entsperren des Laufwerks verwenden:

Wiederherstellungsschlüssel:

016819-571582-437481-136136-091410-684860-468523-035343

Falls der obige Bezeichner nicht mit dem auf dem PC angezeigten Bezeichner übereinstimmt, handelt es sich nicht um den richtigen Schlüssel zum Entsperren des Laufwerks. Versuchen Sie es mit einem anderen Wiederherstellungsschlüssel, oder suchen Sie unter ["http://go.microsoft.com/fwlink/?LinkID=260589"](http://go.microsoft.com/fwlink/?LinkID=260589) nach weiteren Informationen.



## 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: numerisches Kennwort  
Password: benutzerdefiniertes Kennwort  
RecoveryKey: \*.bek komplexer Schlüssel  
StartupKey: gleich wie der RecoveryKey



## Windows Bitlocker einsetzen

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~~