

BitLocker Boot-Pin Lokal aktivieren

Bitlocker aktivieren

Geräte **ohne** TPM:

Zuerst müssen wir BitLocker aktivieren, dazu gehen wir in: "Systemsteuerung -> System und Sicherheit -> BitLocker-Laufwerksverschlüsselung" und gehen auf BitLocker aktivieren.

BitLocker-Laufwerksverschlüsselung

Das Schützen der Laufwerke mit BitLocker trägt dazu bei, Dateien und Ordner vor nicht autorisiertem Zugriff zu schützen.

Betriebssystemlaufwerk

C: BitLocker deaktiviert



 BitLocker aktivieren


Festplattenlaufwerke

Wechseldatenträger - BitLocker To Go

Schließen Sie einen USB-Speicherstick an, um BitLocker To Go zu verwenden.

Danach kommt sicher ein fehler wie dieser hier:



←  BitLocker-Laufwerkverschlüsselung (C:)


BitLocker wird gestartet

- ✗ Auf diesem Gerät kann kein TPM (Trusted Platform Module) verwendet werden. Der Administrator muss für die Richtlinie "Zusätzliche Authentifizierung beim Start anfordern" für Betriebssystemvolumen die Option "BitLocker ohne kompatibles TPM zulassen" festlegen.

[Wie lauten die Systemanforderungen für BitLocker?](#)

Abbrechen

Um diesen Fehler zu umgehen, müssen wir zuerst die Tastenkombination "Windows + R" drücken und dort "" eingeben.

 Ausführen



Geben Sie den Namen eines Programms, Ordners, Dokuments oder einer Internetressource an.

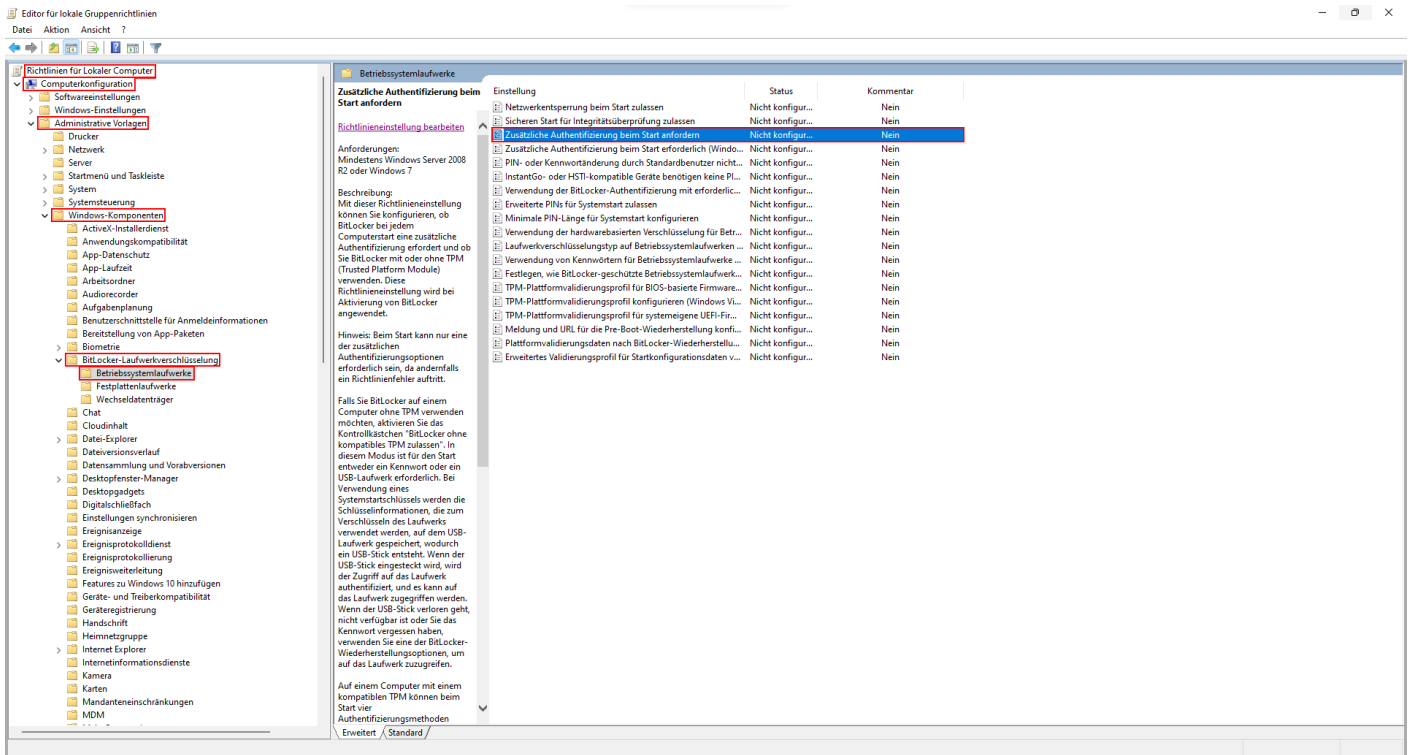
Öffnen:

OK

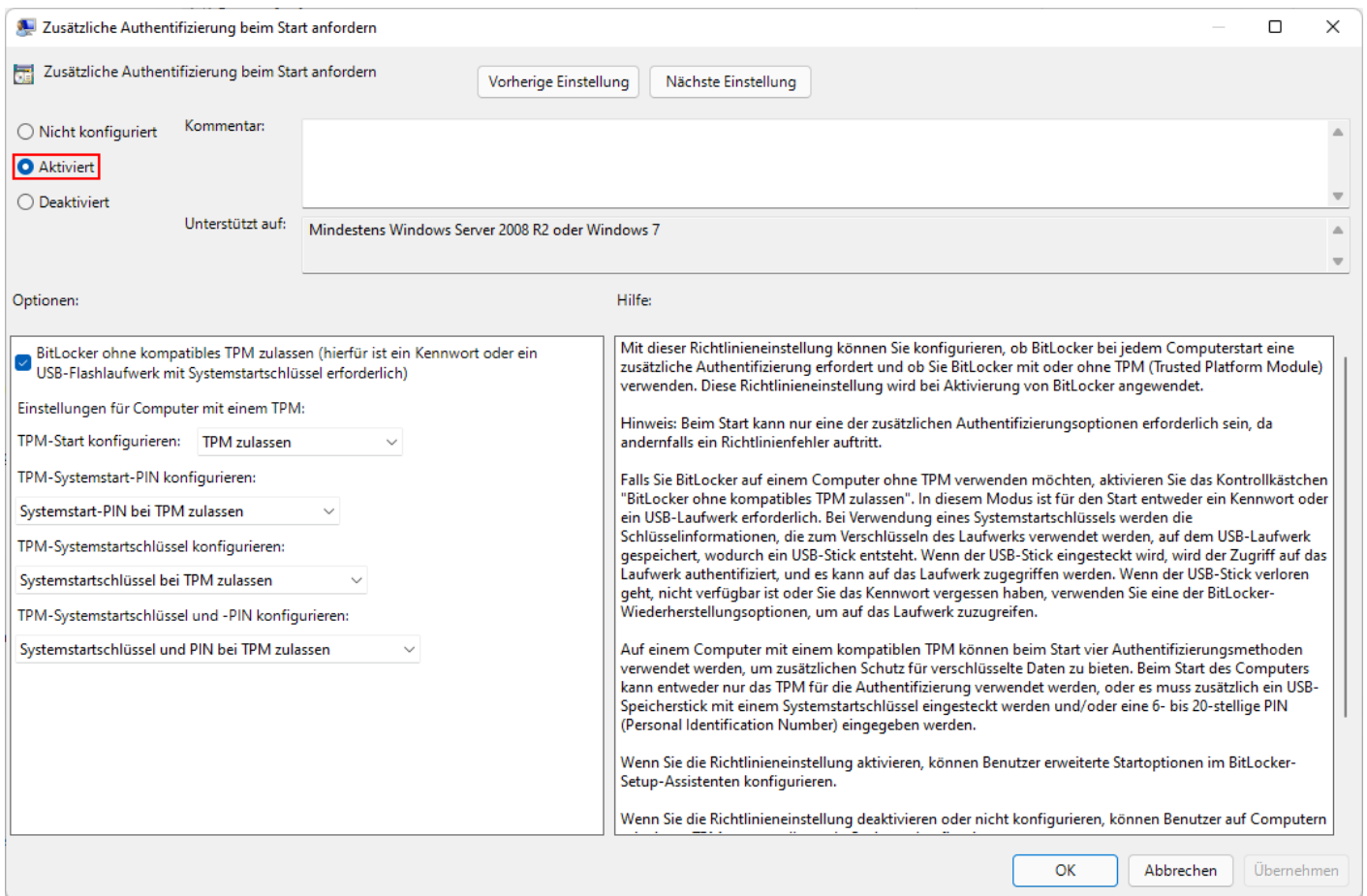
Abbrechen

Durchsuchen...

Danach suchen wir dort in dem "Editor für lokale Gruppenrichtlinien" unter "Richtlinien für Lokaler Computer -> Computerkonfiguration -> Windows-Komponenten -> BitLocker-Laufwerksverschlüsselung -> Betriebssystemlaufwerke" nach der Einstellung "Zusätzliche Authentifizierung beim Start anfordern" und machen darauf ein Doppelklick.



Dann öffnet sich das Fenster "Zusätzliche Authentifizierung beim Start anfordern" dort wählen wir oben Links "Aktiviert" aus, die restlichen Werte können wir so lassen.



Wenn dies erledigt ist, gehen wir zurück in die Systemsteuerung und drücken erneut "**BitLocker aktivieren**". Danach lässt er das TPM Modul Außen vor.

Nun kannst du zwischen einem "**USB-Speicherstick anschließen**" und "**Kennwort eingeben**", der Rest ist selbst erklärend.

Geräte mit TPM:

- Zuerst müssen wir BitLocker aktivieren, dazu gehen wir in: "**Systemsteuerung -> System und Sicherheit -> BitLocker-Laufwerksverschlüsselung**" und gehen auf "**BitLocker aktivieren**".

BitLocker-Laufwerkverschlüsselung

Das Schützen der Laufwerke mit BitLocker trägt dazu bei, Dateien und Ordner vor nicht autorisiertem Zugriff zu schützen.

Betriebssystemlaufwerk

C: BitLocker deaktiviert



 BitLocker aktivieren

Festplattenlaufwerke

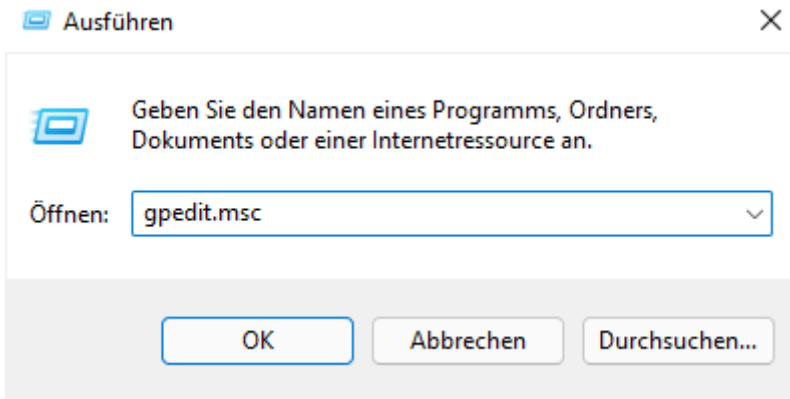
Wechseldatenträger - BitLocker To Go

Schließen Sie einen USB-Speicherstick an, um BitLocker To Go zu verwenden.

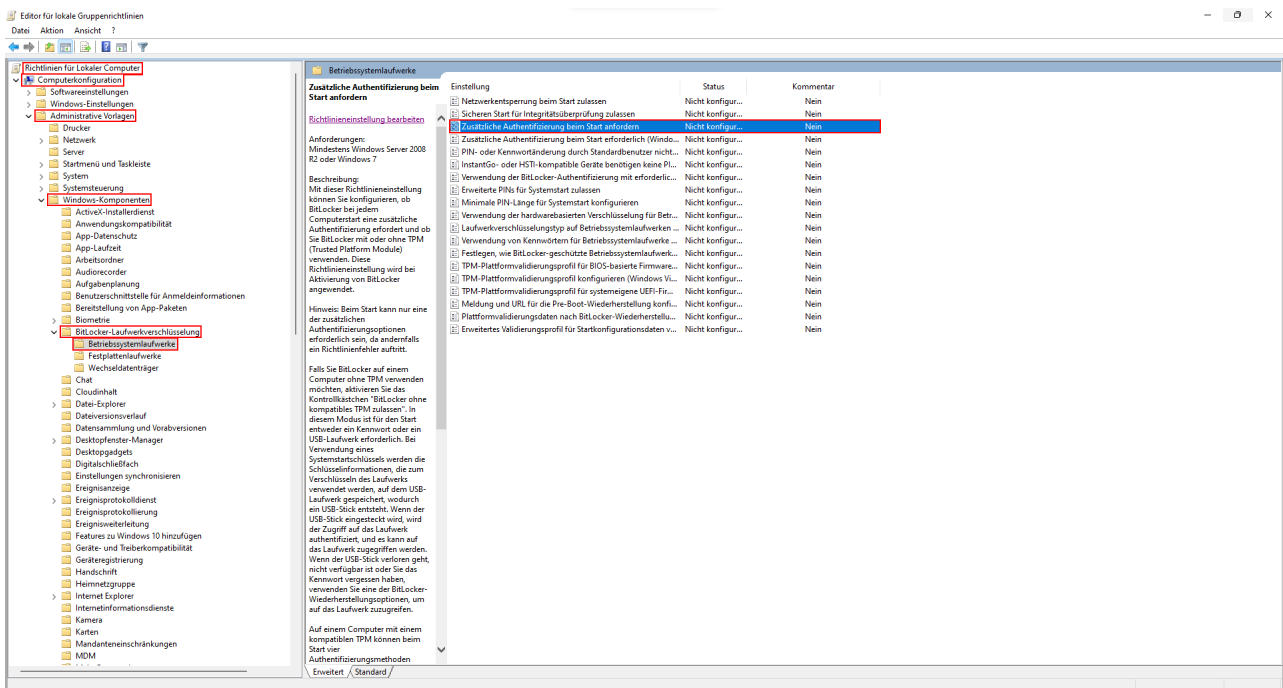
- Wenn BitLocker die Festplatte fertig verschlüsselt und der Computer einen Neustart gemacht hat, können wir weitermachen.

Start PIN aktivieren:

- Als Nächstes drücken "Windows + R" und geben "gpedit.msc" ein.



- Dort unter "Richtlinien für Lokaler Computer -> Computerkonfiguration -> Windows-Komponenten -> BitLocker-Laufwerksverschlüsselung -> Betriebssystemlaufwerke" suchen wir uns die Einstellung "Zusätzliche Authentifizierung beim Start anfordern" und machen darauf ein Doppelklick. Als erstes ändern wir den Status "Nicht konfiguriert" auf "Aktiviert".



- Jenachdem ob ein PIN definitiv benutzt werden soll oder ob dies in den Systemeinstellungen noch geändert werden soll, tragen wir folgendes ein:

Um den PIN definitiv zu verwenden ändern wir in den Optionen den Wert unter "TPM-Systemstart-PIN konfigurieren" von "Systemstart-PIN bei TPM zulassen" auf "Start-PIN bei TPM erforderlich"

Um die Art in der Systemsteuerung noch ändern zu können lassen wir den Wert unter "

TPM-Systemstart-PIN konfigurieren" bei "Systemstart-PIN bei TPM zulassen".

Zusätzliche Authentifizierung beim Start anfordern

☐ Nicht konfiguriert Kommentar:

☒ **Aktiviert**

☐ Deaktiviert

Unterstützt auf: Mindestens Windows Server 2008 R2 oder Windows 7

Optionen:

☒ BitLocker ohne kompatibles TPM zulassen (hierfür ist 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, auf dem USB-Laufwerk gespeichert, wodurch ein USB-Stick entsteht. Wenn der USB-Stick eingesteckt wird, wird der Zugriff auf das Laufwerk authentifiziert, und es kann auf das Laufwerk zugegriffen werden. Wenn der USB-Stick verloren geht, nicht verfügbar ist oder Sie das Kennwort vergessen haben, verwenden Sie eine der BitLocker-Wiederherstellungsoptionen, um auf das Laufwerk zuzugreifen.

Auf einem Computer mit einem kompatiblen TPM können beim Start vier Authentifizierungsmethoden verwendet werden, um zusätzlichen Schutz für verschlüsselte Daten zu bieten. Beim Start des Computers kann entweder nur das TPM für die Authentifizierung verwendet werden, oder es muss zusätzlich ein USB-Speicherstick mit einem Systemstartschlüssel eingesteckt werden und/oder eine 6- bis 20-stellige PIN (Personal Identification Number) eingegeben werden.

Wenn Sie die Richtlinieneinstellung aktivieren, können Benutzer erweiterte Startoptionen im BitLocker-Setup-Assistenten konfigurieren.

Wenn Sie die Richtlinieneinstellung deaktivieren oder nicht konfigurieren, können Benutzer auf Computern ohne TPM keine erweiterten Startoptionen konfigurieren.

OK Abbrechen Übernehmen

- Falls du anstatt einen Nummern PIN auch das Alphabet benutzen willst, änderst du noch die Einstellung "**Erweiterte PINs für Systemstart zulassen**", diese befinden sich ebenfalls unter "**Richtlinien für Lokaler Computer -> Computerkonfiguration -> Windows-Komponenten -> BitLocker-Laufwerksverschlüsselung -> Betriebssystemlaufwerke**".

Diese aktivierst du.

Erweiterte PINs für Systemstart zulassen

☐ Nicht konfiguriert Kommentar:

☒ **Aktiviert**

☐ Deaktiviert

Unterstützt auf: Mindestens Windows Server 2008 R2 oder Windows 7

Optionen:

Hilfe:

Mit dieser Richtlinieneinstellung können Sie konfigurieren, ob erweiterte Systemstart-PINs mit BitLocker verwendet werden.

Erweiterte Systemstart-PINs ermöglichen die Verwendung verschiedener Zeichen, einschließlich Groß- und Kleinbuchstaben, Symbolen, Zahlen und Leerzeichen. Diese Richtlinieneinstellung wird bei Aktivierung von BitLocker angewendet.

Wenn Sie diese Richtlinieneinstellung aktivieren, handelt es sich bei allen neu festgelegten BitLocker-Systemstart-PINs um erweiterte PINs.

Hinweis: Möglicherweise unterstützen nicht alle Computer erweiterte PINs in der PXE (Pre-Boot eXecutive Environment). Benutzern wird dringend empfohlen, während des BitLocker-Setups eine Systemüberprüfung durchzuführen.

Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, werden keine erweiterten PINs verwendet.

- Wer möchte kann auch die Minimale PIN-Länge vorgeben, dazu öffnest du die Einstellung "Minimale PIN-Länge für Systemstart konfigurieren" welche ebenfalls unter "**Richtlinien für Lokaler Computer -> Computerkonfiguration -> Windows-Komponenten -> BitLocker-Laufwerksverschlüsselung -> Betriebssystemlaufwerke**" zu finden ist.

Dazu ändert zu den Status von "Nicht konfiguriert" auf "Aktiviert" und gibst unter den Optionen deine Mindestanzahl von Zeichen an.

Minimale PIN-Länge für Systemstart konfigurieren

Vorherige Einstellung Nächste Einstellung

☐ Nicht konfiguriert Kommentar:

☒ **Aktiviert**

☐ Deaktiviert Unterstützt auf: Mindestens Windows Server 2008 R2 oder Windows 7

Optionen: Hilfe:

Mindestanzahl von Zeichen: 309

Mit dieser Richtlinieneinstellung können Sie eine Mindestlänge für eine TPM-Start-PIN (Trusted Platform Module) konfigurieren. Diese Richtlinieneinstellung wird bei Aktivierung von BitLocker angewendet. Die Start-PIN muss mindestens 4 und darf höchstens 20 Ziffern aufweisen.

Wenn Sie die Richtlinieneinstellung aktivieren, können Sie eine Mindestanzahl von Ziffern für das Festlegen der Start-PIN vorgeben.

Wenn Sie die Richtlinieneinstellung deaktivieren oder nicht konfigurieren, können Benutzer eine Start-PIN mit einer beliebigen Länge von 6 bis 20 Ziffern konfigurieren.

HINWEIS: Wenn die Mindestlänge der PIN unter 6 Ziffern festgelegt ist und eine PIN geändert wird, versucht Windows, die TPM 2.0-Sperrperiode auf einen Wert über dem Standardwert zu aktualisieren. Falls erfolgreich, setzt Windows die TPM-Sperrperiode nur auf den Standardwert zurück, wenn das TPM zurückgesetzt wird.

OK Abbrechen Übernehmen

- Wenn wir nun zurück zu BitLocker in die Systemsteuerung gehen, haben wir nun die Option "**Ändern, wie das Laufwerk beim Start entsperrt wird**".

Betriebssystemlaufwerk

Windows (C:) BitLocker aktiviert



- Schutz anhalten
- Ändern, wie das Laufwerk beim Start entsperrt wird
- Wiederherstellungsschlüssel sichern
- PIN ändern
- BitLocker deaktivieren

Festplattenlaufwerke

Wechseldatenträger - BitLocker To Go

Schließen Sie einen USB-Speicherstick an, um BitLocker To Go zu verwenden.

Jenachdem was du gewählt hast funktioniert die Option oder nicht.

Bei der Wahl von "Start-PIN bei TPM erforderlich" bekommst du nun folgenden Fehler:



BitLocker-Laufwerkverschlüsselung (C:)

Festlegen, wie das Laufwerk beim Start entsperrt werden soll

- Die Gruppenrichtlinieneinstellungen für BitLocker-Startoptionen stehen in Konflikt und können nicht angewendet werden. Weitere Informationen erhalten Sie vom Systemadministrator.

Fertig stellen

- Um nun den PIN / Passwort zu verwenden, musst du eine Administrative CMD öffnen.

Dort gibst du nun `manage-bde -protectors -add c: -TPMAndPIN` ein, im anschluss drückst du

Enter und gibst deinen PIN / Passwort ein.

Um den Status zu überprüfen kannst du in der CMD auch `manage-bde -status` eingeben.

Falls du den PIN ändern willst, kannst du dies entweder in der Systemsteuerung unter BitLocker machen oder per CMD mit dem Befehl `manage-bde -changePIN c:`

Bei der Wahl von "**Systemstart-PIN bei TPM zulassen**" kannst du einfach weiter in der Systemsteuerung unter BitLocker-Laufwerksverschlüsselung machen und dort "**Ändern, wie das Laufwerk beim Start entsperrt wird**" auswählen, der Rest ist selbsterklärend.

Revision #8

Created 5 February 2024 15:10:05 by Julian

Updated 23 September 2024 09:29:33 by Julian