

Windows mit BitLocker verschlüsseln

Mit dieser Anleitung kannst du deinen Laptop mit BitLocker verschlüsseln.

“ Grundlegende Informationen zur Festplattenverschlüsselung unter Windows findest du [hier](#). {.is-info}

“ Bevor du mit der Verschlüsselung startest: Bitte hänge deinen Laptop ans Stromkabel und installiere als erstes alle Windows-Updates. {.is-info}

1. Öffne zunächst die BitLocker Einstellungen, indem du im Startmenü nach `BitLocker` suchst und rechts auf `Öffnen` klickst.

“ Wenn du Windows Home nutzt gibt es bei dir kein BitLocker. Wie du das herausfinden kannst, steht [hier](#). Du findest stattdessen im Startmenü `Geräteverschlüsselung`. Obwohl die Installation weitgehend gleich ist, gibt es wichtige Unterschiede, die du [hier](#) nachlesen kannst. {.is-info}

1-startmenü-bitlocker.png

2. In unserem Beispiel ist BitLocker deaktiviert (Festplatte nicht verschlüsselt). Auf der rechten Seite kannst du `BitLocker aktivieren`.

1-bitlocker-deaktiviert.png

Laptop ohne TPM (Sicherheitschip)

Wenn dein Laptop keinen Sicherheitschip (TPM) enthält, bekommst du an dieser Stelle folgende

Fehlermeldung: `Auf diesem Gerät kann kein TPM verwendet werden. Der Administrator muss für die Richtlinie "Zusätzliche Authentifizierung beim Start anfordern" für Betriebssystemvolumes die Option "BitLocker ohne kompatibles TPM zulassen" festlegen`

Wenn die Fehlermeldung bei dir kommt, nutze [bitte diese Anleitung](#) und springe runter zu `Anleitung: BitLocker ohne TPM aktivieren`.

Keine Fehlermeldung bekommen? Hier geht's weiter!

3. Als nächstes sollst du deinen Wiederherstellungsschlüssel sichern. Was der Wiederherstellungsschlüssel ist wird [hier](#) erklärt. Am besten speicherst du ihn in eine Datei, kopierst ihn dann in deinen Passwort-Manager und löschst die Datei dann von deinem Laptop.

“ Du kannst den Wiederherstellungsschlüssel `in eine Datei speichern`. Allerdings erlaubt es Windows dir nicht, die Datei auf die Festplatte vom Laptop zu speichern. Das ist eine Sicherheitsvorkehrung, da du den Wiederherstellungsschlüssel benötigst, wenn dein Laptop nicht mehr startet. Du kannst ihn z. B. auf einem USB-Stick speichern (unbedingt danach löschen!). Alternativ kannst du ihn auch drucken. Du kannst ihn dann wirklich drucken oder kannst das "in Datei drucken"-Feature nutzen. Du müsstest einen "virtuellen" Drucker auswählen können, mit dem du den Wiederherstellungsschlüssel in eine Datei speichern kannst (und damit auch einfach z. B. auf den Desktop). {.is-info}

Wähle im Assistenten `Wiederherstellungsschlüssel drucken`.

2-wiederherstellungsschlüssel-drucken.png

4. Wähle den (virtuellen) Drucker `in Datei speichern` und wähle einen Ordner deiner Wahl aus, in dem der Wiederherstellungsschlüssel gespeichert werden soll.

3-wiederherstellungsschlüsse-in-datei-drucken.png

So sieht übrigens dein Wiederherstellungsschlüssel aus

ansicht-wiederherstellungsschlüssel.png

Er besteht aus zwei Teilen:

- **Bezeichner:** Er identifiziert deine Festplatte eindeutig und ist hilfreich, wenn du mehrere Wiederherstellungsschlüssel/Laptops sicherst. Die Nummer wird dir angezeigt, wenn du deinen Wiederherstellungsschlüssel eingeben musst.
- **Wiederherstellungsschlüssel:** Das ist das Passwort, mit dem du die Festplatte entschlüsseln kannst. Du solltest ihn geheim halten und an einem sicheren Ort speichern.

5. Wähle als nächstes `Gesamtes Laufwerk verschlüsseln`.

4-gesamtes-laufwerk-verschlüsseln.png

6. Wähle den `neuen Verschlüsselungsmodus`.

5-neue-verschlüsselungsmethode-nutzen.png

7. Aktiviere die `BitLocker-Systemüberprüfung`.

6-systemüberprüfung-aktivieren.png

8. Als nächstes wird dir angezeigt, dass ein `Neustart erforderlich` ist. Die Verschlüsselung beginnt nach dem Neustart automatisch. Starte deinen Laptop neu (vergiss nicht, dir diese Anleitung zu speichern).

7-verschlüsselung-beginnt-nach-neustart.png

9. Nach dem Neustart beginnt die Verschlüsselung automatisch im Hintergrund. Du findest im Systemtray rechts unten (der Pfeil nach oben) ein Symbol für die Verschlüsselung. Wenn du dort drauf klickst, siehst du den Fortschritt der Verschlüsselung.

8-verschlüsselung-läuft.png

9-bitlocker-verschlüsselung-beginnt.png

Es kann etwas dauern bis die Verschlüsselung erfolgreich abgeschlossen ist.

10-bitlocker-verschlüsselung-abgeschlossen.png

10. In den BitLocker-Einstellungen kannst du überprüfen: `C: BitLocker aktiv`. Damit ist deine Festplatte verschlüsselt.

11-bitlocker-ist-aktiviert.png

“ Falls du hier im Fenster zwei Partitionen (z. B. C: und D:) hast, achte darauf dass Bitlocker für alle Partitionen aktiv ist. Wenn du diese Anleitung befolgst ist C:

(das System) verschlüsselt, aber D: (Datenpartition) nicht (falls du eine hast).
{.is-danger}

Als nächstes solltest du unbedingt Pre-Boot Authentication aktivieren. Das ist ein wichtiger zusätzlicher Schutz. Was das genau ist wird [hier](#) beschrieben. Die Anleitung zum Aktivieren findest du [hier](#).

Version #1

Erstellt: 2026-08-07 17:06:38 UTC von RAZ Migration Bot

Zuletzt aktualisiert: 2026-08-07 17:06:38 UTC von RAZ Migration Bot