



Verschlüsselung von Massenspeichermedien

Kurzinformation zur Verschlüsselung beispielsweise eines USB-Sticks

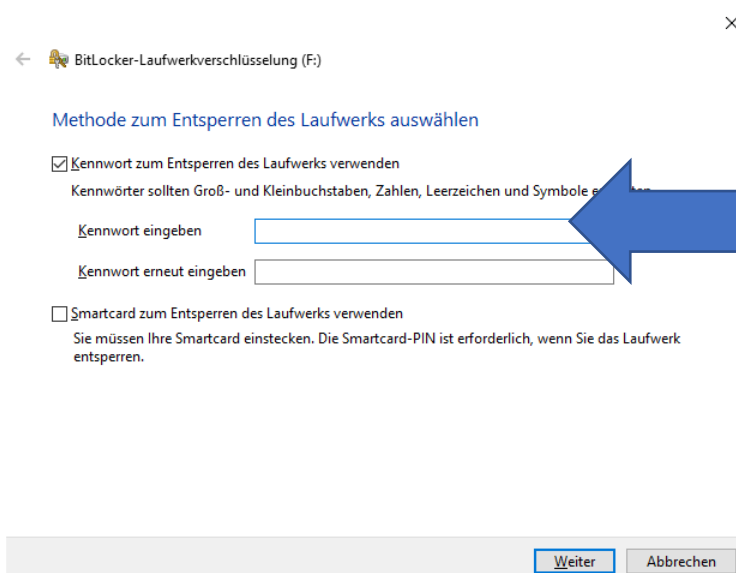
Wir möchten Sie im Folgenden kurz darauf hinweisen, dass USB-Sticks, auf denen sich jegliche Arten von Schülerdaten (Zeugnisse, Lernentwicklungsgespräche etc.) befinden, unbedingt verschlüsselt werden müssen. Um auf seinen Stick zugreifen zu können, muss man ein Kennwort eingeben. Wie Sie Ihren Stick am Schulrechner verschlüsseln können, sehen Sie in der beigefügten Anleitung: „Wie verschlüssele ich einen USB-Stick unter Windows 10?“. Hierbei handelt es sich um ein einfaches Verschlüsselungstool - die BitLockerfunktion von Windows. Dies funktioniert natürlich auch bei externen, sowie internen Festplatten.

Es gibt auch USB-Sticks zu kaufen, die bereits verschlüsselt sind. Alternativ ist das Programm „VeraCrypt Setup 1.19“ ist zur Verschlüsselung zu empfehlen.

Bitte denken Sie auch daran Ihre Daten zu Hause zu schützen. Computer, auf denen vertrauliche Informationen von Schülern und der Schule gespeichert sind, müssen mit einem Kennwort geschützt sein, so dass kein Dritter Zugriff darauf nehmen kann.

Anleitung: Wie verschlüssele ich einen USB-Stick unter WINDWOS 10?

1. USB-Stick einstecken
2. Arbeitsplatz öffnen
3. Mit rechter Maustaste auf den USB-Stick klicken
4. Auf „BitLocker aktivieren“ klicken
→ BitLocker wird gestartet
5. Methode zum Verschlüsseln wählen (Kennwort verwenden), gewünschtes Kennwort eingeben und erneut eingeben, dann auf „Weiter“ klicken





6. Auswählen, wie der Wiederherstellungsschlüssel gespeichert werden soll

← BitLocker-Laufwerkverschlüsselung (F:) ×

Wie soll der Wiederherstellungsschlüssel gesichert werden?

i Einige Einstellungen werden vom Systemadministrator verwaltet.
Wenn Sie das Kennwort vergessen oder die Smartcard verlieren, können Sie mithilfe eines Wiederherstellungsschlüssels auf das Laufwerk zugreifen.

→ In Datei speichern

→ Wiederherstellungsschlüssel drucken

[Wie finde ich später meinen Wiederherstellungsschlüssel?](#)

Weiter Abbrechen

7. Auswählen, wie viel Speicherplatz verschlüsselt werden soll

← BitLocker-Laufwerkverschlüsselung (F:) ×

Auswählen, wie viel Speicherplatz des Laufwerks verschlüsselt werden soll

Bei der Einrichtung von BitLocker auf einem neuen Laufwerk oder PC muss nur der derzeit verwendete Teil des Laufwerks verschlüsselt werden. Beim Hinzufügen neuer Daten werden diese von BitLocker automatisch verschlüsselt.

Falls Sie BitLocker auf einem bereits verwendeten PC oder Laufwerk aktivieren, sollten Sie das gesamte Laufwerk verschlüsseln. Durch die Verschlüsselung des gesamten Laufwerks wird der Schutz aller Daten sichergestellt. Dazu gehören auch gelöschte Daten, die möglicherweise immer noch abrufbare Informationen enthalten.

Nur verwendeten Speicherplatz verschlüsseln (schneller, optimal für neue Computer und Laufwerke)

Gesamtes Laufwerk verschlüsseln (langsamer, aber optimal für PCs und Laufwerke, die bereits verwendet werden)

Weiter Abbrechen



8. Verschlüsselungsmodus wählen

← BitLocker-Laufwerkverschlüsselung (F:) ×

Zu verwendenden Verschlüsselungsmodus auswählen


Mit Windows 10 (Version 1511) wird ein neuer Datenträger-Verschlüsselungsmodus (XTS-AES) eingeführt. Dieser Modus unterstützt zusätzliche Integrität, ist mit älteren Windows-Versionen aber nicht kompatibel.

Bei einem Wechseldatenträger, den Sie mit einer älteren Windows-Version verwenden möchten, sollten Sie den kompatiblen Modus wählen.

Bei einem Festplattenlaufwerk oder einem Laufwerk, das nur mit Geräten eingesetzt wird, auf denen Windows 10 (Version 1511) oder höher ausgeführt wird, sollten Sie den neuen Verschlüsselungsmodus wählen.

Neuer Verschlüsselungsmodus (am besten für Festplattenlaufwerke auf diesem Gerät geeignet)

Kompatibler Modus (am besten für Laufwerke geeignet, die von diesem Gerät entfernt werden können)



9. Mit der Verschlüsselung starten


← BitLocker-Laufwerkverschlüsselung (F:) ×

Möchten Sie das Laufwerk jetzt verschlüsseln?

Das Laufwerk kann mithilfe eines Kennworts entspert werden.

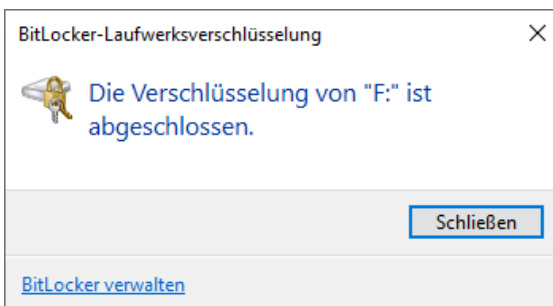
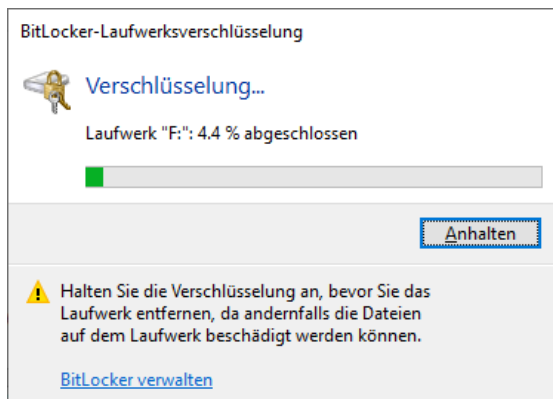
Die Verschlüsselung kann abhängig von der Größe des Laufwerks einige Zeit in Anspruch nehmen.

Bis zum Abschluss der Verschlüsselung werden die Dateien nicht geschützt.

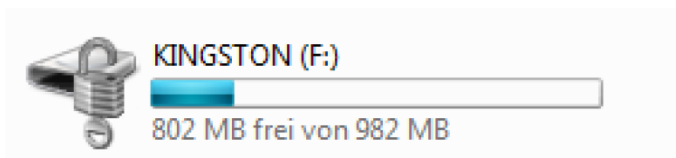




10. Verschlüsselung wird gestartet und dauert ein paar Minuten (nachdem man nach einer Wiederherstellungsdatei gefragt wurde)



11. USB-Stick ist verschlüsselt und kann nach dem Einstecken nur mit dem Kennwort gelesen werden





Anleitung: Wie nutze ich den verschlüsselten USB-Stick?

Steckt man den USB-Stick wieder in ein Gerät ein, muss man das Kennwort eingeben und auf „Entsperren“ klicken

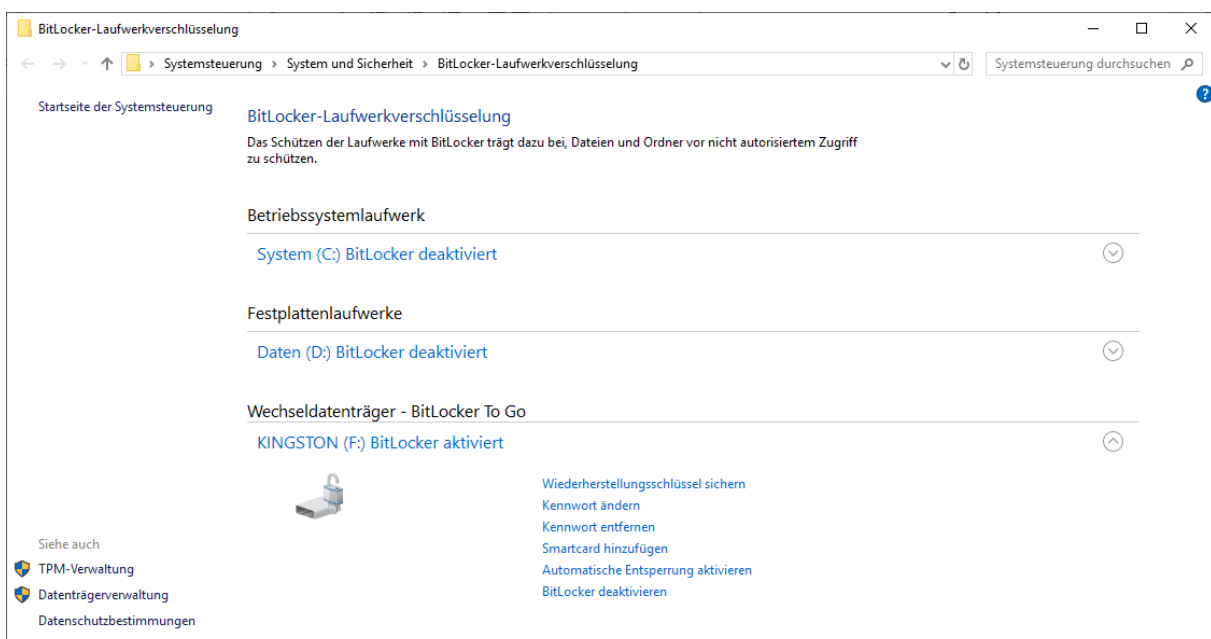
BitLocker (F:)

Geben Sie das Kennwort ein, um dieses Laufwerk zu entsperren.

Um optimale Sicherheit zu gewährleisten, sollte bei jeder Benutzung das Kennwort eingegeben werden und das Feld „Auf diesem PC automatisch entsperren“ nicht verwendet werden.

Anleitung: Wie ändere ich das Kennwort des verschlüsselten Sticks?

1. USB-Stick einstecken
2. Arbeitsplatz öffnen
3. Mit rechter Maustaste auf das Laufwerk klicken
→ „Bitlocker verwalten“ auswählen
4. „Kennwort ändern“ auswählen





5. Kennwort eingeben und auf „Weiter“ klicken

BitLocker-Laufwerkverschlüsselung (F:)

Kennwort ändern

Sie sollten ein sicheres Kennwort erstellen, das Groß- und Kleinbuchstaben, Zahlen, Symbole und Leerzeichen enthält. Kennwörter können 8 bis 256 Zeichen lang sein.

Altes Kennwort

Neues Kennwort

Neues Kennwort bestätigen

[Vergessenes Kennwort zurücksetzen](#)

[Wie wähle ich ein sicheres Kennwort aus?](#)

BitLocker-Laufwerkverschlüsselung (F:)

Kennwort ändern

Sie sollten ein sicheres Kennwort erstellen, das Groß- und Kleinbuchstaben, Zahlen, Symbole und Leerzeichen enthält. Kennwörter können 8 bis 256 Zeichen lang sein.

Altes Kennwort

Neues Kennwort

Neues Kennwort bestätigen

[Vergessenes Kennwort zurücksetzen](#)

[Wie wähle ich ein sicheres Kennwort aus?](#)

i Das Kennwort wurde erfolgreich geändert.