



1. Klicken Sie mit der rechten Maustaste auf Ihren Datenträger (z.B. Laufwerk C:)

2. Wählen Sie zuerst die Variante, mit der Ihr Laufwerk entsperrt werden soll. Wir empfehlen die Variante per Kennwort-Eingabe.



Abbrechen

- 3. Geben Sie das Kennwort ein, was Sie zum entsperren des Notebooks nutzen wollen.
- 4. Bestätigen Sie es durch erneute Eingabe.

	X
🔶 🏘 BitLocker-Laufwerkverschlüsselung (C:)	
Kennwort zum Entsperren des Laufwerks erstellen	
Sie sollten ein sicheres Kennwort erstellen, das Groß- und Kleinbuchstaben, Zahlen, Leerzeichen enthält.	Symbole und
Kennwort eingeben	
3	
Kennwort erneut eingeben	
4	
Tipps zum Erstellen eines sicheren Kennworts	
Wei	ter Abbrechen

5. Für den Fall, dass Sie das Kennwort vergessen sollten, erstellt das System einen Wiederherstellungsschlüssel. Diesen Speichern Sie bitte auf dem verbundenen USB-Stick.

		×
÷	Ref BitLocker-Laufwerkverschlüsselung (C:)	
	Wie soll der Wiederherstellungsschlüssel gesichert werden?	
	 Einige Einstellungen werden vom Systemadministrator verwaltet. 	
	Ein Wiederherstellungsschlüssel kann für den Zugriff auf Dateien und Ordner verwendet werden, falls Sie Ihren PC nicht entsperren können. Es wird empfohlen, mehrere Wiederherstellungsschlüssel getrennt von PC aufzubewahren.	n
	ightarrow In Microsoft-Konto speichern	
5	→ Auf USB-Speicherstick speichern	
	\rightarrow In Datei speichern	
	→ Wiederherstellungsschlüssel drucken	
	Wie finde ich später meinen Wiederherstellungsschlüssel?	
	Weiter Abbrechen	

Hinweis:

Beim Verschlüsselungsprozess werden Sie aufgefordert, den geheimen Wiederherstellungsschlüssel entweder externen abzuspeichern oder auszudrucken. Bitte speichern Sie diesen geheimen Wiederherstellungsschlüssel auf einem sicheren Medium ab und bewahren diesen an einem sehr sicheren Ort.

Bei Verlust des Wiederherstellungsschlüssel ist es leider nicht mehr möglich das Geräte zu entsperren, auch nicht dem Support.

In solch einem Fall müsste das Gerät komplett neu installiert werden. Hierbei gehen alle auf dem Gerät gespeicherten Daten verloren!

6. Wählen Sie den USB-Stick aus, der Ihnen in der Liste angezeigt wird und klicken Sie auf "Speichern".



×

 \sim

Weiter Abbrechen

7. Für größtmögliche Sicherheit verschlüsseln Sie nun bitte das gesamte Laufwerk.

÷	RitLocker-Laufwerkverschlüsselung (C:)
	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.
7	 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. Hierfür wählen Sie den neuen Verschlüsselungsmodus.

<u>ACHTUNG:</u> Wenn Sie einen Wechseldatenträger wie beispielsweise eine USB-Festplatte verschlüsseln möchten, der auch an anderen Geräten zum Einsatz kommt, dann wählen Sie bitte den Kompatiblen Modus als Verschlüsselungsmodus.

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. Di Neuer Verschlüsselungsmodus (am besten für Festplattenlaufwerke auf diesem Gerät geeignet)	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)	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) Mompatibler Modus (am besten für Laufwerke geeignet, die von diesem Gerät entfernt werden können)	RitLocker-Laufwerkverschlüsselung (C:)
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.	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. P Neuer Verschlüsselungsmodus (am besten für Festplattenlaufwerke auf diesem Gerät geeignet) O Kompatibler Modus (am besten für Laufwerke geeignet, die von diesem Gerät entfernt werden können)	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)	Zu verwendenden Verschlüsselungsmodus auswählen
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.	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)	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)	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 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)	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) Compatibler Modus (am besten für Laufwerke geeignet, die von diesem Gerät entfernt werden können)	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) O Kompatibler Modus (am besten für Laufwerke geeignet, die von diesem Gerät entfernt werden können)	Bei einem Wechseldatenträger, den Sie mit einer älteren Windows-Version verwenden möchten, sollten Sie den kompatiblen Modus wählen.
) Neuer Verschlüsselungsmodus (am besten für Festplattenlaufwerke auf diesem Gerät geeignet)	Neuer Verschlüsselungsmodus (am besten für Festplattenlaufwerke auf diesem Gerät geeignet) O Kompatibler Modus (am besten für Laufwerke geeignet, die von diesem Gerät entfernt werden können)	Neuer Verschlüsselungsmodus (am besten für Festplattenlaufwerke auf diesem Gerät geeignet) Kompatibler Modus (am besten für Laufwerke geeignet, die von diesem Gerät entfernt werden können)	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.
	O Kompatibler Modus (am besten für Laufwerke geeignet, die von diesem Gerät entfernt werden können)	🕜 Kompatibler Modus (am besten für Laufwerke geeignet, die von diesem Gerät entfernt werden können)) Neuer Verschlüsselungsmodus (am besten für Festplattenlaufwerke auf diesem Gerät geeignet)

9. Schließen Sie den Assistenten für die Laufwerksverschlüsselung ab, indem Sie auf weiter klicken.



10.Da die Verschlüsselung des Laufwerks einen Neustart benötigt, führen Sie diesen Neustart bitte aus.



11.Sie werden bereits während des Neustarts aufgefordert, Ihr Laufwerk zu entschlüsseln.

ACHTUNG: Diese Aufforderung wird nun bei jedem Neustart ergehen.

Geben Sie das Kennwort zum Entsperren dieses Laufwerks ein.
Drücken Sie die EINFG-Taste, um das Kennwort bei Eingabe anzuzeigen.
Drücken Sie zum Fortfahren die Fingabetaste
Drücken Sie ESC, um die BitLocker-Wiederherstellung auszuführen.

12.Nachdem Ihr System erfolgreich hochgefahren wurde, beginnt die eigentliche Verschlüsselung des Laufwerks. Den Status des Verschlüsselungsvorganges können Sie abrufen, indem Sie in der Taskleiste das Icon mit der linken Maustaste doppelklicken.



13.Die Verschlüsselung ist erfolgreich durchgeführt, wenn 100% erreicht sind. Anschließend wird Ihnen das Laufwerk als verschlüsselt im System angezeigt.

