

Konfiguration Microsoft BitLocker (Laufwerksverschlüsselungstool) gesamtes Laufwerk

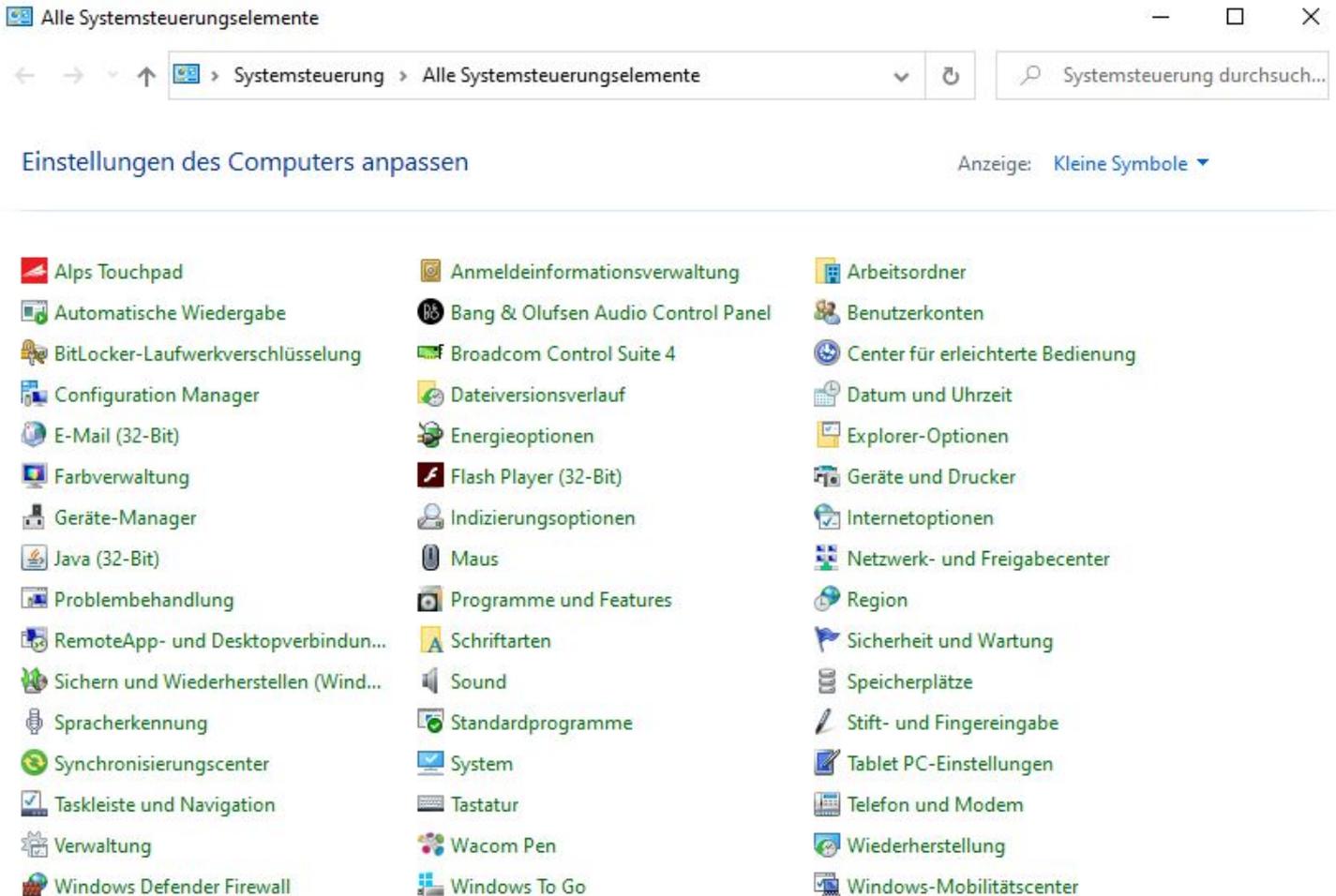
Publiziert it-support@fhnw.ch allgemeine Anleitung Benutzerdokumentation

BitLocker, Laufwerksverschlüsselungstool, gesamtes Laufwerk

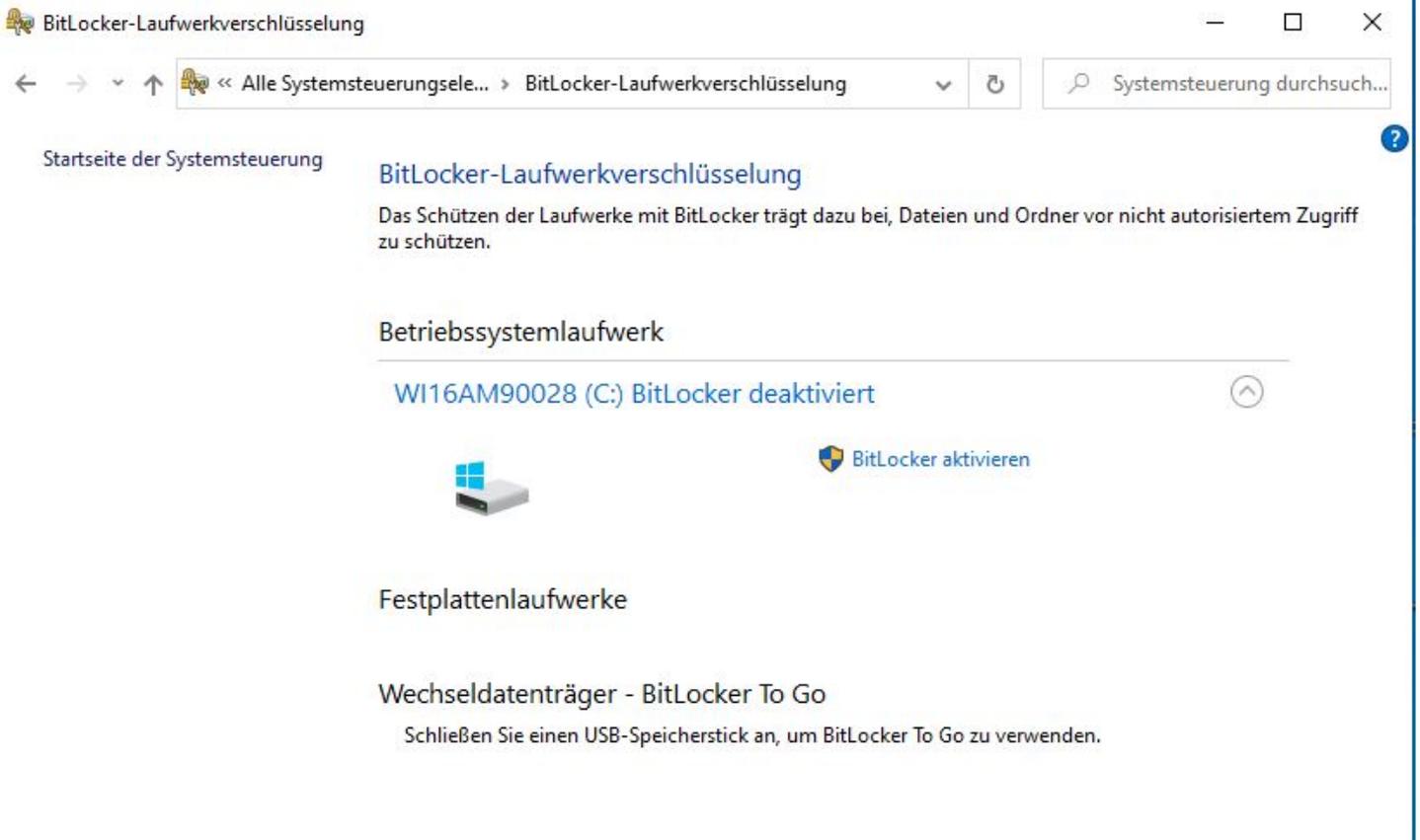
Da das Laufwerksverschlüsselungstool "BitLocker" von Microsoft Kostenfrei und Vorinstalliert mit Windows 10 zur Verfügung steht, ist eine Installation nicht von Nöten.

Folgende Schritte dienen zur Aktivierung von BitLocker Laufwerksverschlüsselung für das Gesamte Windows Laufwerk.

1. Öffnen der Systemsteuerung

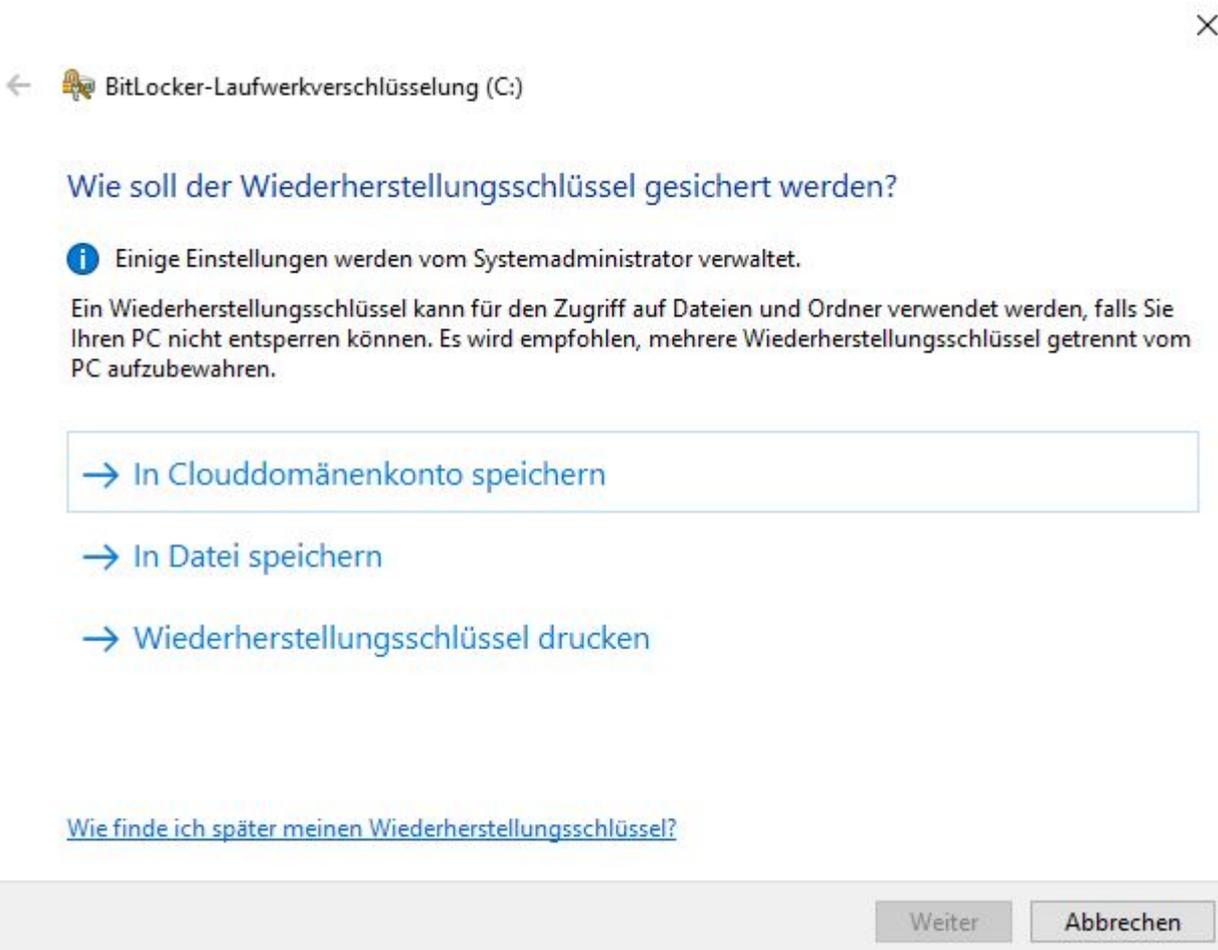


2. Auswählen "BitLocker-Laufwerksverschlüsselung"



3. BitLocker aktivieren

WICHTIG: Zum aktivieren ist der .admin erforderlich!



4. Sicherung des Wiederherstellungsschlüssels

WICHTIG: Die Sichere Aufbewahrung des Wiederherstellungsschlüssels ist WICHTIG, ohne diesen Wiederherstellungsschlüssels kann das Laufwerk NICHT Entschlüsselt werden

BitLocker-Wiederherstellungsschlüssel speichern unter

Dieser PC > FHNW (S:) > dennis.lueckefett

Organisieren Neuer Ordner

Name	Änderungsdatum	Typ	Größe
_FHNW	23.11.2016 16:24	Dateiordner	
Benutzerdefinierte Office-Vorlagen	26.01.2017 12:38	Dateiordner	
Library	28.05.2015 10:23	Dateiordner	
Neuer Ordner	05.07.2019 13:06	Dateiordner	
Sicherung	05.07.2019 13:07	Dateiordner	
WINDOWS	29.01.2016 11:11	Dateiordner	
Windows-TrueType	17.02.2015 10:48	Dateiordner	
BitLocker-Wiederherstellungsschlüssel A...	03.04.2020 14:54	Textdokument	2 KB

Dateiname: BitLocker-Wiederherstellungsschlüssel 8576D71E-36FF-46BB-AB2D-7D4845BD22FE.TXT

Dateityp: Textdateien (*.txt)

Speichern Abbrechen

5. Auswählen welcher Bereich Verschlüsselt werden soll

BitLocker-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.

- 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

6. Auswählen des zu Verwendeten Verschlüsselungsmodus



←  BitLocker-Laufwerkverschlüsselung (C:)

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)

Weiter

Abbrechen

7. BitLocker Laufwerksverschlüsselung starten

Vorab kann eine BitLocker-Systemüberprüfung ausgeführt werden. Dies ist NICHT Zwingend erforderlich!



←  BitLocker-Laufwerkverschlüsselung (C:)

Möchten Sie das Laufwerk jetzt verschlüsseln?

Je nach Größe des Laufwerks dauert der Verschlüsselungsvorgang unter Umständen eine Weile.

Sie können Ihre Arbeit fortsetzen, während das Laufwerk verschlüsselt wird. Die Leistung des Computers kann jedoch eingeschränkt sein.

BitLocker-Systemüberprüfung ausführen

Die Systemüberprüfung stellt sicher, dass BitLocker die Wiederherstellungs- und Verschlüsselungsschlüssel richtig lesen kann, bevor das Laufwerk verschlüsselt wird.

Der Computer wird von BitLocker vor der Verschlüsselung neu gestartet.

Hinweis: Diese Prüfung kann einige Zeit dauern, wird jedoch empfohlen, um sicherzustellen, dass die ausgewählte Methode zum Entsperren ohne Wiederherstellungsschlüssel funktioniert.

Verschlüsselung starten

Abbrechen

WICHTIG: Die BitLocker Laufwerksverschlüsselung läuft im Hintergrund. Es kann normal weitergearbeitet werden!

publiziert: 26. April 2020 14:38 Service: S0006 - Fileserver