Konfiguration Microsoft BitLocker (Laufwerksverschlüsselungstool) gesamtes Laufwerk

Publiziert <u>it-support@fhnw.ch</u> 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.



💷 Alle Systemste	euerungselemente						×
$\leftarrow \rightarrow - \uparrow$	Systemsteuerung > Alle Systemsteuerungselemente	~	Ū	Q	Systemsteueru	ng durch	such

Einstellungen des Computers anpassen

Anzeige: Kleine Symbole 🔻

📥 Alps Touchpad	Anmeldeinformationsverwaltung	📱 Arbeitsordner
📷 Automatische Wiedergabe	🚯 Bang & Olufsen Audio Control Panel	😹 Benutzerkonten
RitLocker-Laufwerkverschlüsselung	🖙 Broadcom Control Suite 4	🕲 Center für erleichterte Bedienung
🛼 Configuration Manager	🖉 Dateiversionsverlauf	Datum und Uhrzeit
E-Mail (32-Bit)	Energieoptionen	Explorer-Optionen
💶 Farbverwaltung	Flash Player (32-Bit)	💼 Geräte und Drucker
📇 Geräte-Manager	🔒 Indizierungsoptionen	🔂 Internetoptionen
🕌 Java (32-Bit)	Maus	🚏 Netzwerk- und Freigabecenter
Problembehandlung	Programme und Features	🔗 Region
🐻 RemoteApp- und Desktopverbindun	A Schriftarten	🏲 Sicherheit und Wartung
🐌 Sichern und Wiederherstellen (Wind	M Sound	Speicherplätze
🖶 Spracherkennung	Standardprogramme	🖉 Stift- und Fingereingabe
Synchronisierungscenter	🔛 System	Tablet PC-Einstellungen
Taskleiste und Navigation	Tastatur	🧱 Telefon und Modem
🔆 Verwaltung	🚏 Wacom Pen	🕢 Wiederherstellung
P Windows Defender Firewall	🏪 Windows To Go	Windows-Mobilitätscenter

2. Auswählen "BitLocker-Laufwerksverschlüsselung"

	steuerungsele > BitLocker-Laufwerkverschlusselung V Systemsteuerung			
rtseite der Systemsteuerung	BitLocker-Laufwerkverschlüsselung Das Schützen der Laufwerke mit BitLocker trägt dazu bei, Dateien und Ordner vor nicht autorisiertem zu schützen.			
	Betriebssystemlaufwerk			
	WI16AM90028 (C:) BitLocker deaktiviert			
	BitLocker aktivieren			
	Festplattenlaufwerke			
	Wechseldatenträger - BitLocker To Go Schließen Sie einen USB-Speicherstick an um Bitl ocker To Go zu verwenden.			
icker aktivieren				
G: Zum aktivieren ist der .\admin	n erforderlich!			
	×			
	chlüsselung (C:)			
BitLocker-Laufwerkvers				
Wie soll der Wiederh	nerstellungsschlüssel gesichert werden?			
 BitLocker-Laufwerkvers Wie soll der Wiederh Einige Einstellungen wieder 	rerstellungsschlüssel gesichert werden? erden vom Systemadministrator verwaltet.			
 BitLocker-Laufwerkvers Wie soll der Wiederh Einige Einstellungen w Ein Wiederherstellungsschl Ihren PC nicht entsperren k PC aufzubewahren. 	nerstellungsschlüssel gesichert werden? rerden vom Systemadministrator verwaltet. lüssel kann für den Zugriff auf Dateien und Ordner verwendet werden, falls Sie können. Es wird empfohlen, mehrere Wiederherstellungsschlüssel getrennt vom			
 BitLocker-Laufwerkvers Wie soll der Wiederh Einige Einstellungen w Ein Wiederherstellungsschl Ihren PC nicht entsperren k PC aufzubewahren. 	nerstellungsschlüssel gesichert werden? erden vom Systemadministrator verwaltet. lüssel kann für den Zugriff auf Dateien und Ordner verwendet werden, falls Sie können. Es wird empfohlen, mehrere Wiederherstellungsschlüssel getrennt vom enkonto speichern			
 BitLocker-Laufwerkvers Wie soll der Wiederh Einige Einstellungen w Ein Wiederherstellungsschl Ihren PC nicht entsperren k PC aufzubewahren. In Clouddomäne In Datei speicher 	nerstellungsschlüssel gesichert werden? erden vom Systemadministrator verwaltet. lüssel kann für den Zugriff auf Dateien und Ordner verwendet werden, falls Sie können. Es wird empfohlen, mehrere Wiederherstellungsschlüssel getrennt vom enkonto speichern rn			

Weiter

Abbrechen

4. Sicherung des Wiederherstellungsschlüssels

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

RitLocker-Wiederherstellungsschlüssel speichern unter

	<u>^</u>				-
Dieser PC	Name	Änderungsdatum	Тур	Größe	
3D-Objekte	FHNW	23.11.2016 16:24	Dateiordner		
Bilder	📙 Benutzerdefinierte Office-Vorlagen	26.01.2017 12:38	Dateiordner		
Desktop	Library	28.05.2015 10:23	Dateiordner		
Dokumente	Neuer Ordner	05.07.2019 13:06	Dateiordner		
Developed	Sicherung	05.07.2019 13:07	Dateiordner		
Downloads	WINDOWS	29.01.2016 11:11	Dateiordner		
Musik		17.02.2015 10:48	Dateiordner		
Videos	BitLocker-Wiederherstellungsschlüssel A	03.04.2020 14:54	Textdokument	2 KB	
WI16AM90028 ((
CD-Laufwerk (D:					
evento\$ (\\asara					
FHNW (S:)					
~					
Detains and Ditlas	ker Wiederberstellungsschlüssel 0576D71E 26EE 4	600 AD20 70404500220			
Dateiname:	Renviedemerstellungsschlusser 6570D/TE-30FF-4	000-A020-7040406022F	LAAI		

5. Auswählen welcher Bereich Verschlüsselt werden soll

X

X

Reference 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.

(e) 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

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 f
ür Laufwerke geeignet, die von diesem Ger
ät entfernt werden k
önnen)

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.

X

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