Miten suojata USB-asema tai muistitikku BitLockerilla

USB-asema tai muistitikku voidaan suojata Windows-koneessa BitLocker-toiminnolla. BitLocker on Microsoftin ohjelmisto, joka salaa USB-aseman tai muistitikun siten, että kaikki sinne tallennetut tiedostot salataan automaattisesti ja niiden avaamiseen tarvitaan salausvaiheessa asettamasi salasana.

1. Salauksen asettaminen

- 1. Liitä USB-levy tai -muistitikku Windows-tietokoneeseen.
- 2. Klikkaa Windows-valikko **H** auki ja kirjoita *BitLocker*. Valitse *Manage BitLocker*. Klikkaa USBlevyasemasi tai -tikkusi kohdalla *Ota BitLocker käyttöön* (*Turn on BitLocker*).

Removable data drives - BitLocke	r To Go
KINGSTON (D:) BitLocker off	
-	Turn on BitLocker

 Keksi vahva salasana ja kirjoita se muistilapulle joko kokonaan tai osittain. Katso Kyberturvallisuuskeskuksen ohje. Säilytä lappu turvallisessa paikassa. Kirjaa tieto niin, ettei siitä ulkopuoliselle selviä, minkä palvelun tai kenen salasanasta on kyse, jos lappu katoaa. Jos salasana unohtuu tai häviää, USB-levyn salausta ei saa avattua mitenkään, vaan kaikki sille tallennetut tiedostot on menetetty pysyvästi. Säilytä lappu turvallisessa paikassa. Kirjaa tieto niin, ettei siitä ulkopuoliselle selviä, minkä palvelun tai kenen salasanasta on kyse, jos lappu katoaa.

Klikkaa Poista aseman lukitus salasanan avulla (Use a password to unlock this drive), syötä keksimäsi salasana ja klikkaa Seuraava (Next).

	×
🔶 🎭 BitLocker Drive Encryption (D:)	
Choose how you want to unlock this drive	
Use a password to unlock the drive	
Passwords should contain uppercase and lowercase letters, numbers, spaces, and symbols.	
Enter your password	
Reenter your password	
Use my smart card to unlock the drive	
You'll need to insert your smart card. The smart card PIN will be required when you unlock the drive.	
Next Cance	el

4. Seuraavaksi sinulla on mahdollisuus tallentaa palautusavaimen sisältävä tiedosto tai tulostaa palautusavain. Sen avulla voit avata USB-aseman BitLocker-salauksen, jos unohdat äsken luomasi salasanan. Koska USB-aseman salaus on avattavissa tämän tiedoston avulla, sen saa tallentaa vain riittävän turvalliseen paikkaan. Tätä tiedostoa ei saa tallentaa salaamattomaan paikkaan itse omistamallesi tietokoneelle, mihinkään pilvipalveluun tai muistitikulle.

- a. Keskitetysti ylläpidetyllä TUNI Windows -tietokoneella: Tämän tiedoston tallentaminen tai avaimen tulostaminen on pakollista. TUNIkotihakemisto verkkoasemalla P: on salattu turvallinen tallennuspaikka. Muualla kuin kampusverkossa saat sen käyttöösi käynnistämällä TUNI VPN:n. Klikkaa *Tallenna tiedostoon* (*Save to a file*) ja tallenna palautusavaimen sisältävä tiedosto P:lle.
- b. Muilla tietokoneilla:

Tämän tiedoston tallentaminen ei ole pakollista. Jos sinulla ei ole käytettävissäsi salattua turvallista tallennuspaikkaa, on turvallisempaa, kun et tallenna palautusavaimen sisältävää tiedostoa. Jos sinulla on mahdollisuus tulostaa palautusavain paperille, tee niin.

5. Klikkaa Seuraava (Next).

		×
~	🏘 BitLocker Drive Encryption (D:)	
	How do you want to back up your recovery key?	
	 Your recovery key has been saved. 	
	If you forget your password or lose your smart card, you can use your recovery key to access your drive.	
	\rightarrow Save to a file	
	\rightarrow Print the recovery key	
	How can I find my recovery key later?	
	Next Cance	

 Jos USB-asema on tyhjä, valitse ensimmäinen valinta. Muussa tapauksessa valitse toinen vaihtoehto. Huomaa, että toisella vaihtoehdolla salaaminen kestää hyvin kauan, vaikka muistitikku on tyhjä: noin 2 minuuttia gigatavua kohden tyypillisellä kannettavalla tietokoneella ja muistitikulta. Klikkaa Seuraava (Next).

	X
←	🎭 BitLocker Drive Encryption (D:)
	 BitLocker Drive Encryption (D:) Choose how much of your drive to encrypt If you're setting up BitLocker on a new drive or a new PC, you only need to encrypt the part of the drive that's currently being used BitLocker encrypts new data automatically as you add it. If you're enabling BitLocker on a PC or drive that's already in use, consider encrypting the entire drive. Encrypting the entire drive ensures that all data is protected—even data that you deleted but that might still contain retrievable info. Encrypt used disk space only (faster and best for new PCs and drives) Encrypt entire drive (slower but best for PCs and drives already in use)
	Next Cancel

7. Klikkaa Aloita salaus (Start encrypting).



8. Odota, että salaus valmistuu. Jos sinulla ei ole nyt aikaa odottaa salauksen valmistumista, vaan haluat jatkaa sitä myöhemmin, voit napsauttaa *Keskeytä (Pause)*.

BitLocker Drive Encryption	
R	Encrypting Drive D: 21.5% Completed
	Pause
Pause encryption before removing the drive or files on the drive could be damaged.	
M	anage BitLocker

9. Jos napsautit *Keskeytä (Pause)*, salaus pysähtyy ja sitten voit poistaa USB-aseman tietokoneesta vahingoittamatta tietoja. Jos poistat USB-aseman, voit kytkeä sen myöhemmin tietokoneeseen ja jatkaa salausta klikkaamalla *Jatka (Resume)*.



10. Kun liität USB-aseman Windows-tietokoneeseen, sinua pyydetään antamaan sen BitLockersalasana, jonka määrittelit kohdassa 3. Jos käyttämäsi tietokone on keskitetysti ylläpidetty TUNI Windows -tietokone, voit klikata *Lisää asetuksia (More options)* ja valita *Poista lukitus automaattisesti tässä tietokoneessa (Automatically unlock in this computer)*. Jos teet näin, antamasi salasana tallennetaan turvallisesti tähän tietokoneeseen, eikä sinun tarvitse syöttää sitä uudelleen, kun liität tämän USB-aseman tähän tietokoneeseen. Syötä sitten salasana ja klikkaa *Avaa (Unlock)*.

BitLocker (D:)
Enter password to unlock this drive.
•
More options
Unlock
BitLocker (D:)
Enter password to unlock this drive.
Fewer options
Enter recovery key
Automatically unlock on this PC
Unlock

11. Jos salaus oli keskeytettynä, saat saman ikkunan, jossa olit vaiheessa 9 ja voit jatkaa salausta napsauttamalla *Jatka (Resume)* -painiketta.

Näiden vaiheiden jälkeen USB-asema on salattu, ja voit tallentaa tiedot turvallisesti siihen. Huomaa, että erityisen arkaluontoisten tietojen, kuten GDPR:n 9 artiklassa määriteltyjen erityisten tietoryhmien, tallentamiseen sinun on käytettävä ylimääräistä salausohjelmistoa, kuten Cryptomator tai VeraCrypt. Ota yhteyttä IT Helpdeskiin tarpeen mukaan.

2. Salauksen poistaminen

Voit poistaa USB-asemalle tai muistitikulle asettamasi salauksen seuraavilla ohjeilla.

1. Klikkaa Windows-valikko **H** auki ja kirjoita *BitLocker*. Valitse *Manage BitLocker*. Klikkaa USBlevyasemasi tai -tikkusi kohdalla *Poista BitLocker käytöstä (Turn off BitLocker)*.



2. Klikkaa Poista BitLocker käytöstä (Turn off BitLocker).

BitLocker Drive Encryption	×
Turn off BitLocker	
Your drive will be decrypted. This might take a long t you can keep using your PC during the decryption p	ime, but rocess.

3. Odota, että salaus puretaan. Jos sinulla ei ole nyt aikaa odottaa salauksen valmistumista, vaan haluat jatkaa sitä myöhemmin, voit napsauttaa *Keskeytä (Pause)*.

BitLock	ter Drive Encryption
	Decrypting
6.	Drive D: 90.1% Completed
	Pause
🛕 Pa th	ause decryption before removing the drive or files on e drive could be damaged.
M	lanage BitLocker

4. Jos napsautit *Keskeytä (Pause)*, salauksen purkaminen pysähtyy ja sitten voit poistaa USBaseman tietokoneesta vahingoittamatta tietoja. Jos poistat USB-aseman, voit kytkeä sen myöhemmin tietokoneeseen ja jatkaa salauksen purkamista.



5. Kun toiminto ilmoittaa olevansa valmis, USB-levyasema tai -tikku ei enää ole salattu ja sen tiedostoja voi käyttää ilman salasanaa. Klikkaa *Sulje (Close)*.

