Encrypted Removable Media

(BitLocker to Go)

Encryption is an effective method of protecting data stored on portable USB devices such as flash drives and external hard drives.

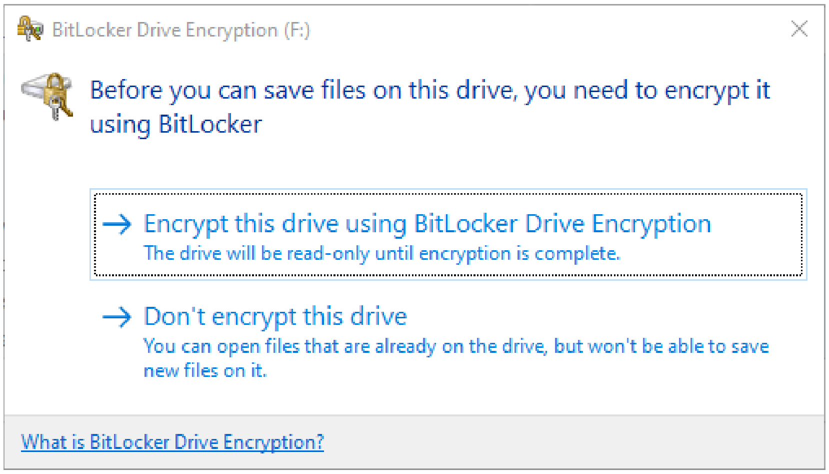
Encryption encodes data so that it can only be read by someone who has the right encryption key (password) to decode it. This means that if your device is lost or stolen, the information contained on it cannot be accessed by unauthorized users.

BitLocker to Go is a feature of Windows 10 (Pro & Enterprise) that allows you to easily encrypt your personal devices and prevent unauthorized access. Without the encryption key, the device is inaccessible.

When you connect your BitLocker encrypted USB device to a Windows PC you will be prompted for your password. After entering the password correctly, you can read and write to your device as normal.

Gulf Coast State College 'Staff' computers protect contents written to removable media with Windows BitLocker to Go Encryption. The following prompt will appear upon inserting an "unencrypted" USB drive into a 'Protected Computer"

- Unencrypted is any removable USB storage device not encrypted with BitLocker
- Protected Computer is any 'Staff' GC domain joined computer with the applied Group Policy for BitLocker



BitLocker Drive Encryption (F:)

Before you can save files on this drive, you need to encrypt it using BitLocker

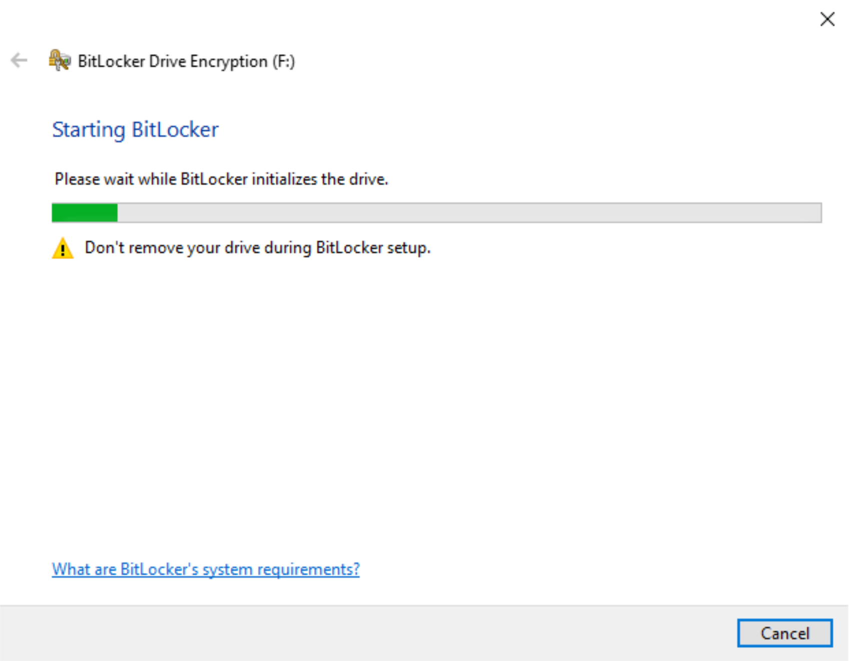
→ Encrypt this drive using BitLocker Drive Encryption
The drive will be read-only until encryption is complete.

→ Don't encrypt this drive
You can open files that are already on the drive, but won't be able to save new files on it.

What is BitLocker Drive Encryption?

If the option to proceed without encrypting '**Don't encrypt this drive**', the contents will be accessible like any other USB drive but the user will not be able to create, edit or save any files on or too the USB storage.

If the option to Encrypt this drive using BitLocker Drive Encryption is selected, the process as outlined below will begin.


BitLocker Drive Encryption (F:)

Starting BitLocker

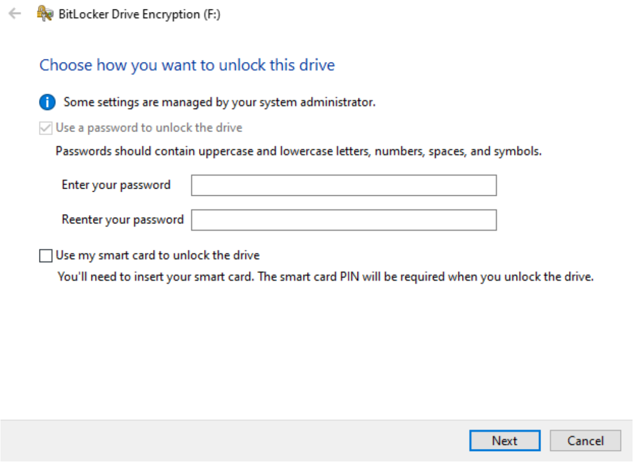
Please wait while BitLocker initializes the drive.

Don't remove your drive during BitLocker setup.

What are BitLocker's system requirements?

You will be prompted for a 16-character minimum password. The password being set will be used anytime the USB drive is plugged into any computer in order to access the contents

The 16-character password does not need to be complex or include any special characters, we recommend using a favorite quote, a sentence or a combination of different word like: horse + battery + staple (password being: **horsebatterystaple**)


BitLocker Drive Encryption (F:)

Choose how you want to unlock this drive

Some settings are managed by your system administrator.

☑ Use a password to unlock the drive

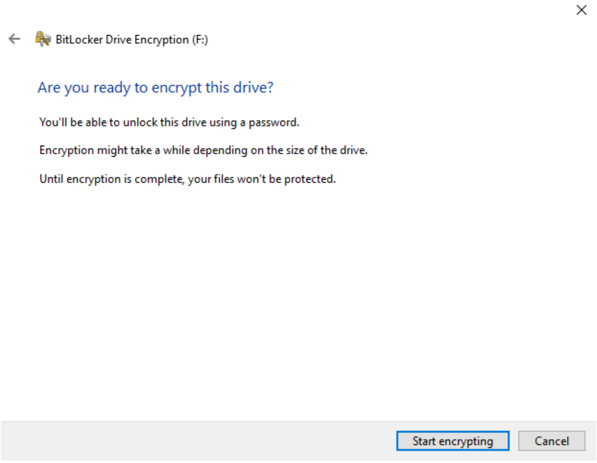
Passwords should contain uppercase and lowercase letters, numbers, spaces, and symbols.

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.


BitLocker Drive Encryption (F:)

Are you ready to encrypt this drive?

You'll be able to unlock this drive using a password.

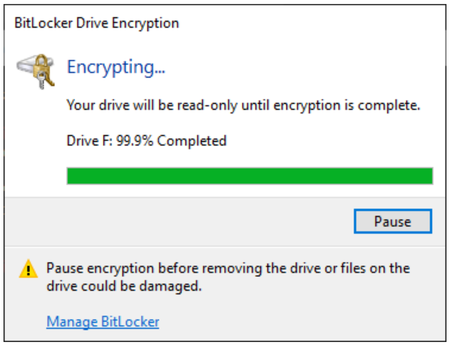
Encryption might take a while depending on the size of the drive.

Until encryption is complete, your files won't be protected.

After inputting the password and selecting ‘Start Encrypting’ the process will start.

The time to complete encryption will vary depending on how much contents is already on the USB drive. If there is little to no data, it should be less than a minute to complete.

Meanwhile data on the drive is still accessible while the drive is being encrypted, however do not unplug the USB drive until the encryption process is complete.



BitLocker Drive Encryption

Encrypting...

Your drive will be read-only until encryption is complete.

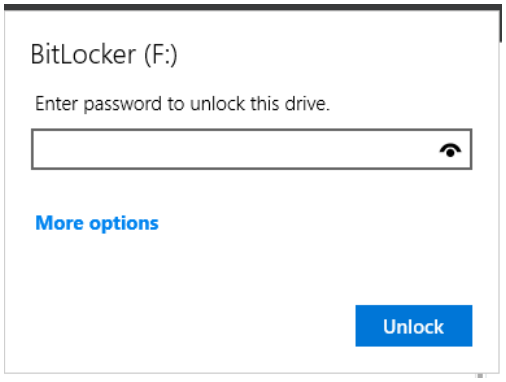
Drive F: 99.9% Completed

Pause encryption before removing the drive or files on the drive could be damaged.

Once encryption is complete, the USB drive can be removed.

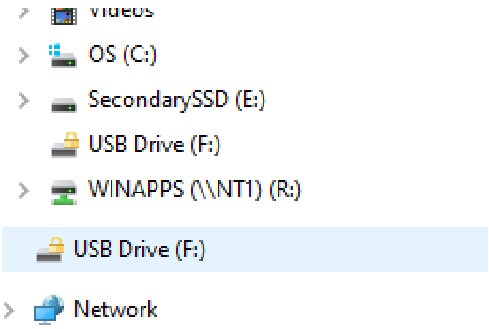
Moving forward anytime the USB drive is inserted into a computer it will prompt for the ‘set’ password to Unlock the drive. (See below)

Once Unlocked the USB drive will be accessible with Read / Write capability



BitLocker (F:)

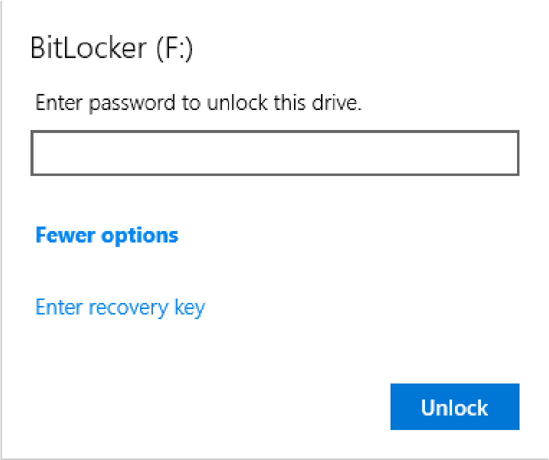
Enter password to unlock this drive.



If a user happened to ‘forget’ the password for their USB and needed assistance from ITS, this can be done is certain cases.

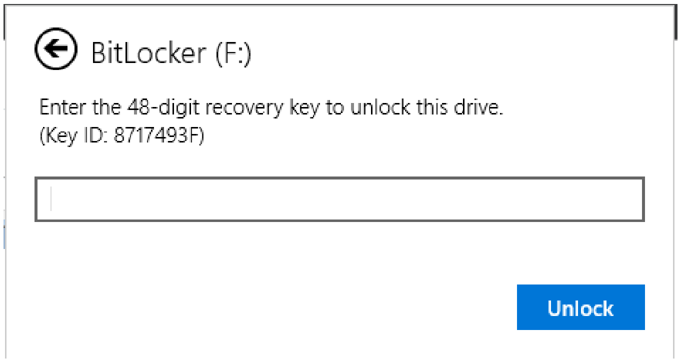
By clicking ‘More Options’ exposes an option to Enter a Recovery Key, this recovery ‘**Key ID**’ can be provided to ITS and they can in turn help recover and access the USB

NOTE This is only an option the USB drive was encrypted from a **GCSC Staff workstation,** *note classroom PC’s, Smart Stations, etc. are not ‘Staff’ workstations*



BitLocker (F:)

Enter password to unlock this drive.



BitLocker (F:)

Enter the 48-digit recovery key to unlock this drive.
(Key ID: 8717493F)

Items to be mindful of with BitLocker Encryption:

- You will always be prompted to encrypt an unprotected removable drive (USB drive); encryption is not necessary to read existing files.

- ITS **cannot** assist with or recover any USB drives encrypted from a non-GCSC computer (*e.g. personal, public, etc.*)

- Bitlocker'd USB storage cannot be accessed on Mac OS or Linux without the use of 3rd party software or apps such as **UUBYTE BitLocker Geeker** (MacOS), **SYSGeeker Bitlocker Reader** (MacOS), or **Dislocker** (Linux). ITS does not provide support for accessing USB storage on non-Windows operating systems.