HOW to QUICKLY and PERMANENTLY SANITIZE ANY DRIVE (SSD, USB thumb drive or standard hard drive)

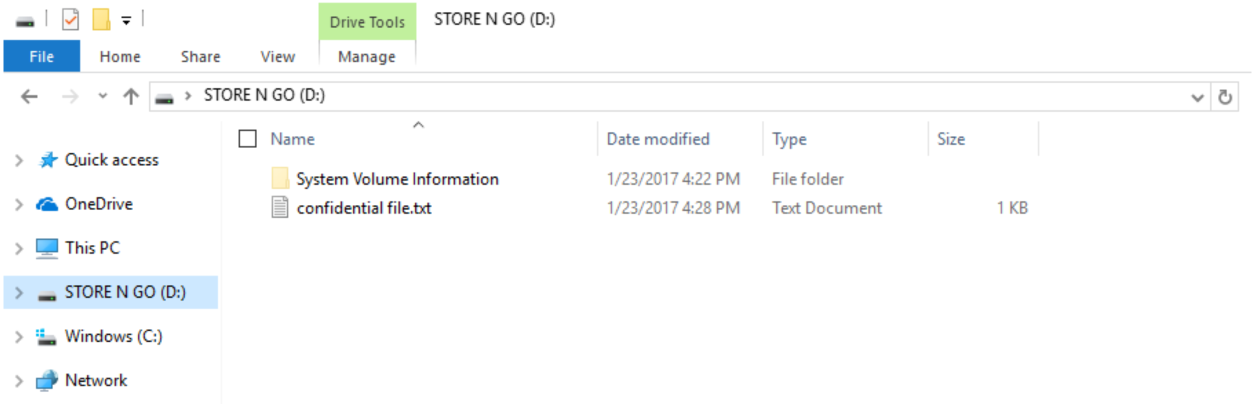
This document will show how to sanitize media and ensure no data can be recovered. We will do this by doing four steps.

1. We will use the Windows tool BitLocker to encrypt the drive.
2. We will then format the drive.
3. We will then re-encrypt the drive one final time. By re-encrypting it a second time, the encryption key from Step 1 will be overwritten, rendering the encrypted data from the first encryption unrecoverable, and leaving the drive with random, meaningless data.
4. We will format the drive one more time. This will leave the drive ready for future reuse.

Step 1.

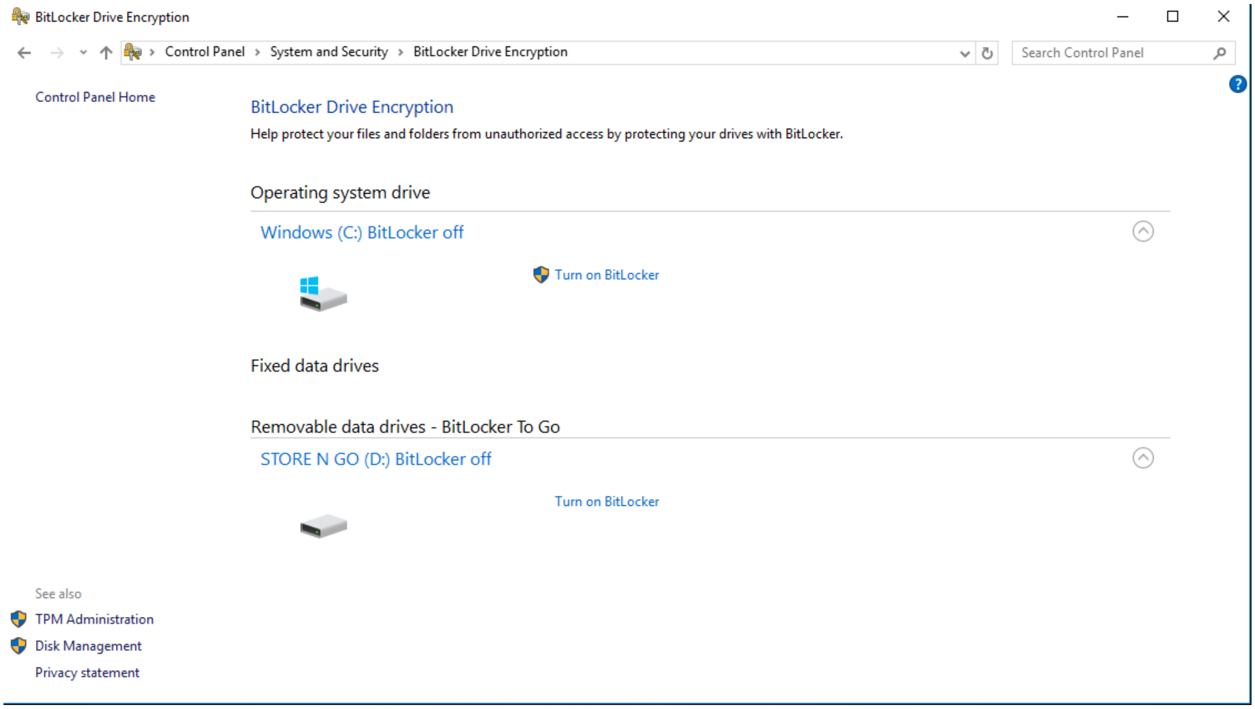
Connect the drive to your system and enable BitLocker on it.

In this example, we have a thumb drive with some confidential data on it. We want to ensure that no one can ever recover this data. You can see this in Windows Explorer. In this example, the drive is D:.



Name	Date modified	Type	Size
System Volume Information	1/23/2017 4:22 PM	File folder	
confidential file.txt	1/23/2017 4:28 PM	Text Document	1 KB

Open BitLocker (Click *Search* and run bitlocker or Control Panel\System and Security\BitLocker Drive Encryption). Note: you may need administrative privileges to run BitLocker.



BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

Operating system drive

Windows (C:) BitLocker off

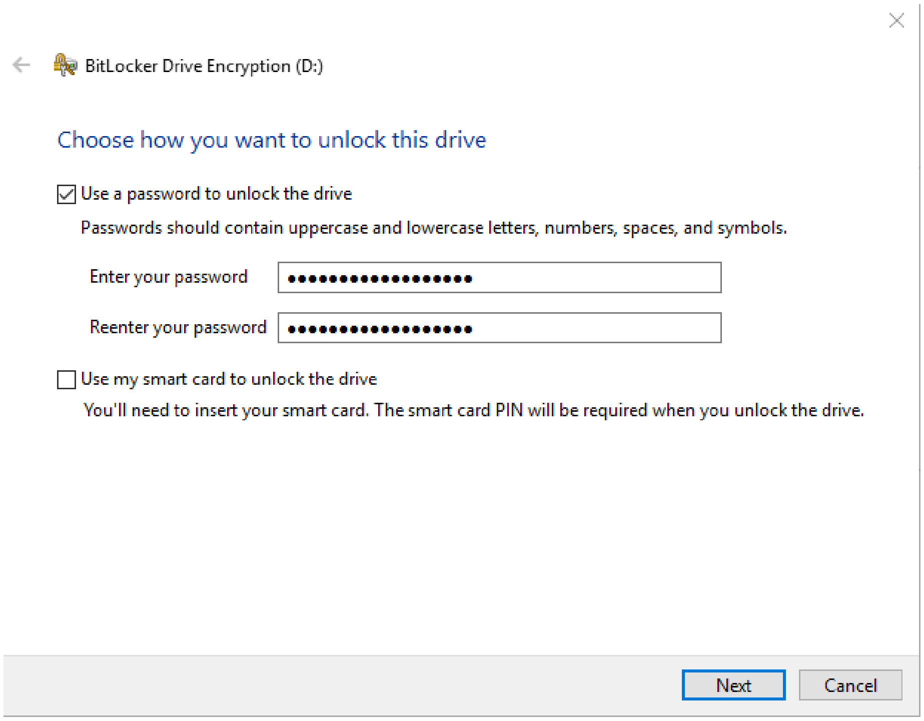
Fixed data drives

Removable data drives - BitLocker To Go

STORE N GO (D:) BitLocker off

Click *Turn on BitLocker* (Do not do this on your C: drive unless you want to encrypt your C: drive)

Set up a password to unlock the drive. Use any random characters. You will not need to remember this password, so it can be anything.



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.

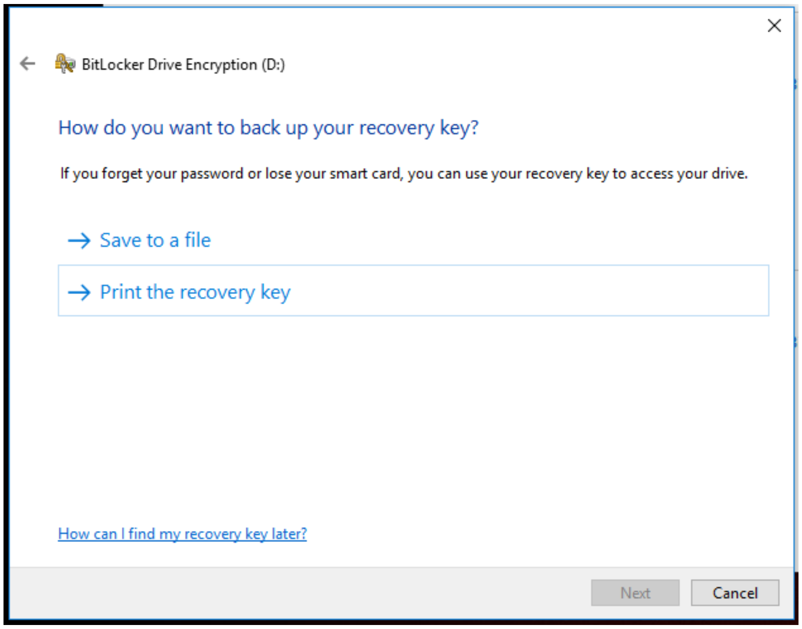
Enter your password ●●●●●●●●●●●●●●●●●

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.

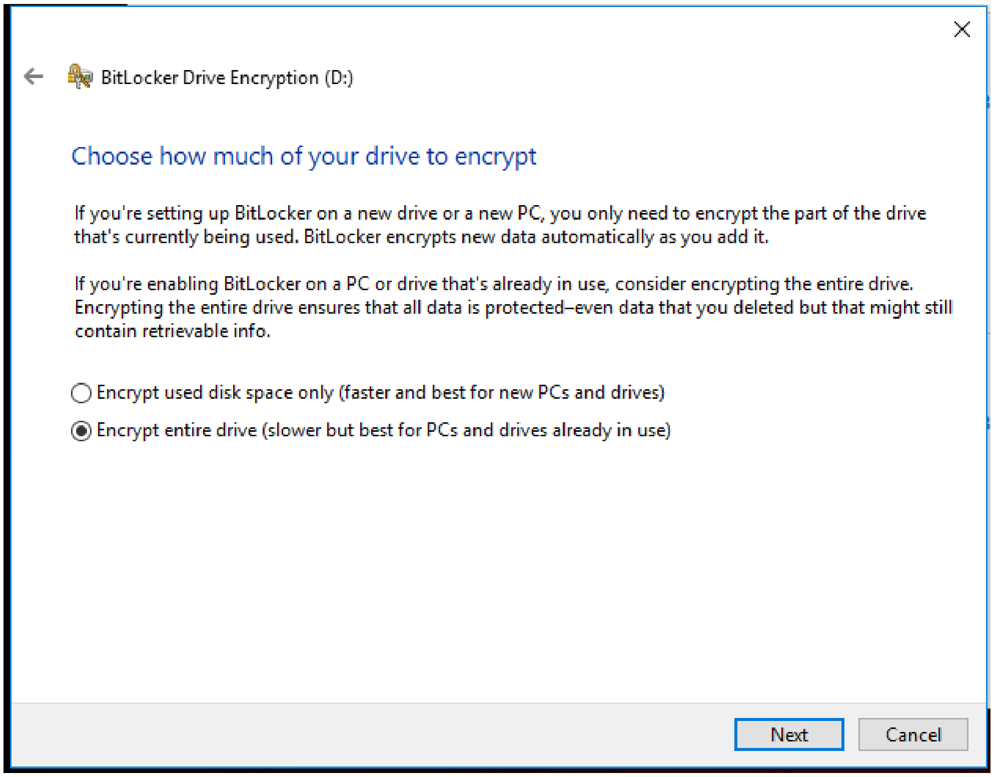
When prompted to save or print the recovery key either save it to a location other than the media you are sanitizing or print it out and shred the paper. I suggest saving it to an alternate location, then deleting the file after it is saved.


BitLocker Drive Encryption (D:)

How do you want to back up your recovery key?

If you forget your password or lose your smart card, you can use your recovery key to access your drive.

When prompted to Choose how much of your drive to encrypt, choose to encrypt the entire drive. This will ensure that any deleted files or data remaining on the drive are also encrypted.


BitLocker Drive Encryption (D:)

Choose how much of your drive to encrypt

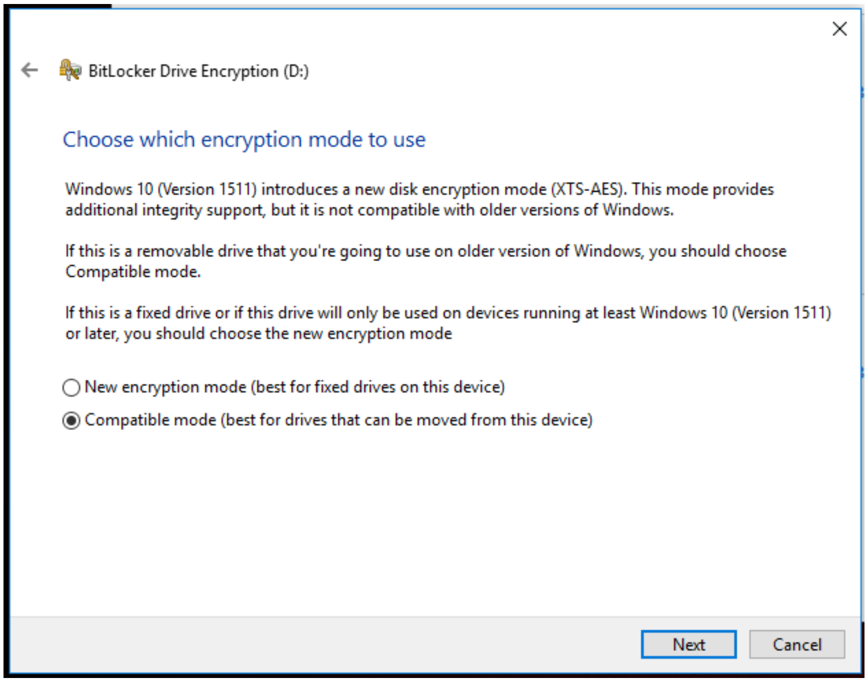
If you're setting up BitLocker on a new drive or a new PC, you only need to encrypt the part of the drive that's currently being used. BitLocker encrypts new data automatically as you add it.

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)

If running this on Windows 10 operating system, you will be prompted to choose an encryption mode. Choose either mode, it doesn't matter since we will be formatting this drive shortly.



BitLocker Drive Encryption (D:)

Choose which encryption mode to use

Windows 10 (Version 1511) introduces a new disk encryption mode (XTS-AES). This mode provides additional integrity support, but it is not compatible with older versions of Windows.

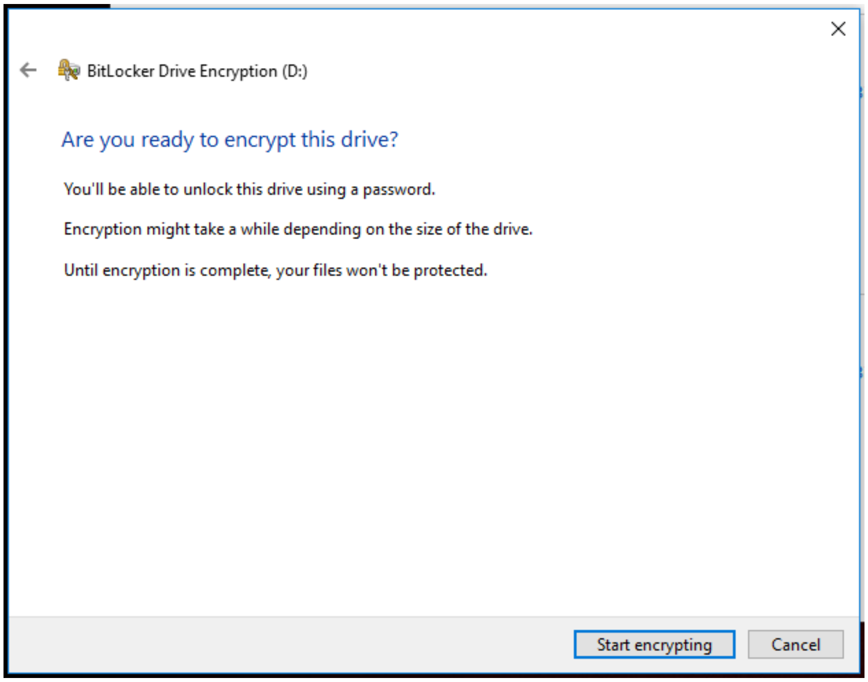
If this is a removable drive that you're going to use on older version of Windows, you should choose Compatible mode.

If this is a fixed drive or if this drive will only be used on devices running at least Windows 10 (Version 1511) or later, you should choose the new encryption mode

○ New encryption mode (best for fixed drives on this device)

● Compatible mode (best for drives that can be moved from this device)

Click *Start encrypting* when to start the encryption process.



BitLocker Drive Encryption (D:)

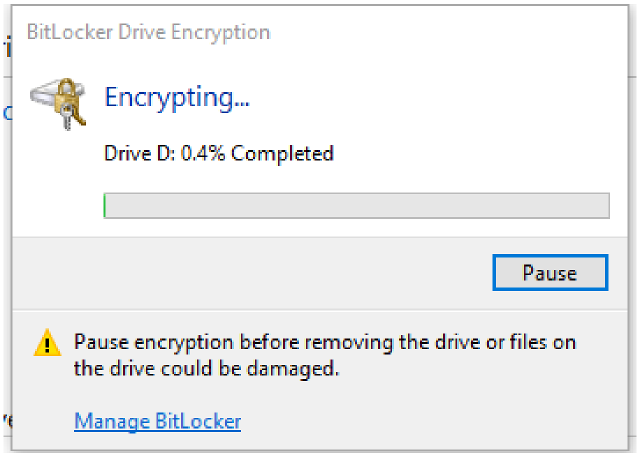
Are you ready to encrypt this drive?

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.

Wait for the encryption to complete.


BitLocker Drive Encryption

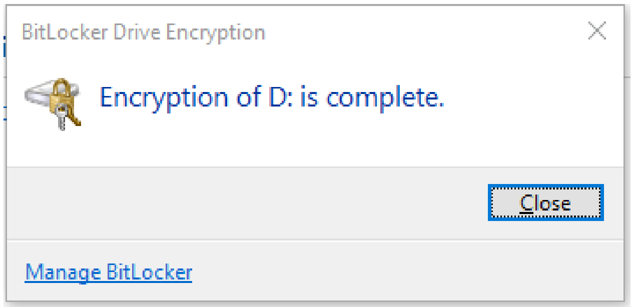
Encrypting...

Drive D: 0.4% Completed

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

Note that this can take quite a while.

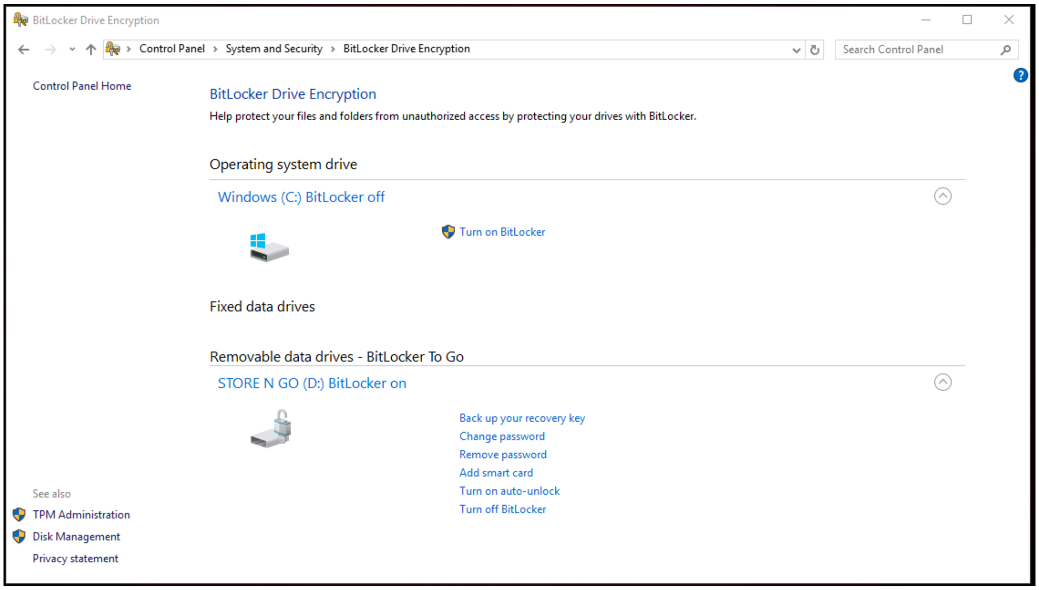
Once finished, you will get the following message:


BitLocker Drive Encryption

Encryption of D: is complete.

You can close BitLocker.

You will now see that BitLocker is on:


BitLocker Drive Encryption

BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

Operating system drive

Windows (C:) BitLocker off

Fixed data drives

Removable data drives - BitLocker To Go

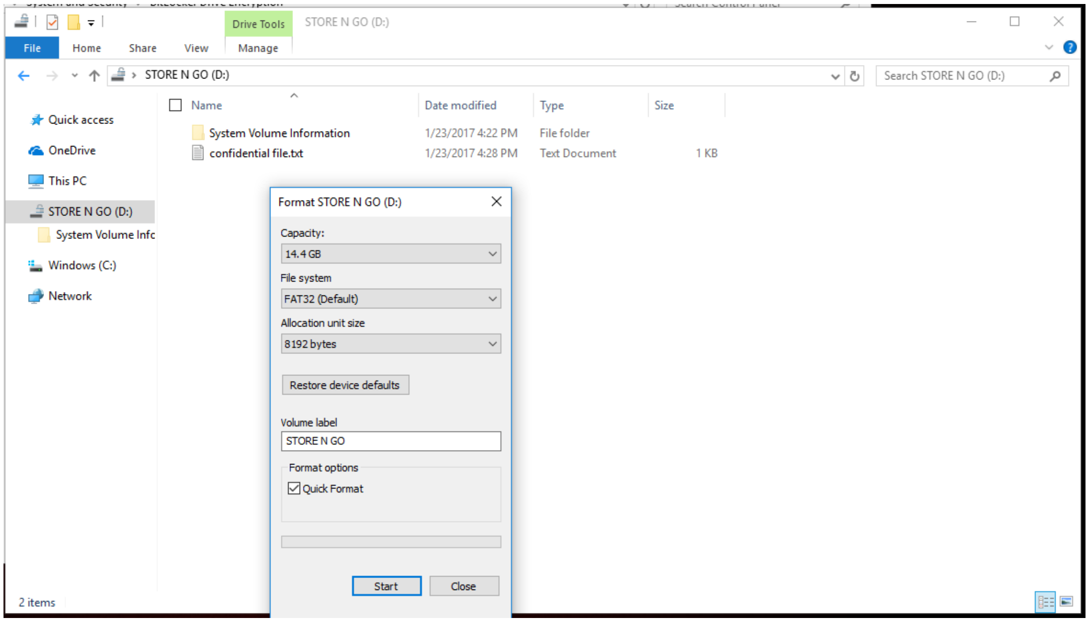
STORE N GO (D:) BitLocker on

Step 2:

Format the drive.

Open Windows explorer, right click on the drive (D: in this case) and choose format.

You can choose a Quick Format if you like.



Name	Date modified	Type	Size
System Volume Information	1/23/2017 4:22 PM	File folder	
confidential file.txt	1/23/2017 4:28 PM	Text Document	1 KB

Format STORE N GO (D:)

Capacity:
14.4 GB

File system
FAT32 (Default)

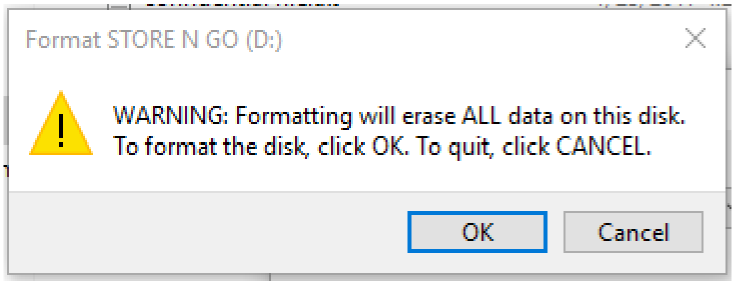
Allocation unit size
8192 bytes

Volume label
STORE N GO

Format options
☑ Quick Format

Click *Start*.

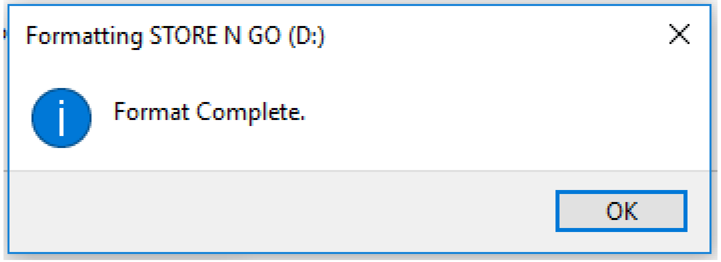
When prompted with the warning that formatting the disk will erase all data on the disk, choose *OK*.



Format STORE N GO (D:)

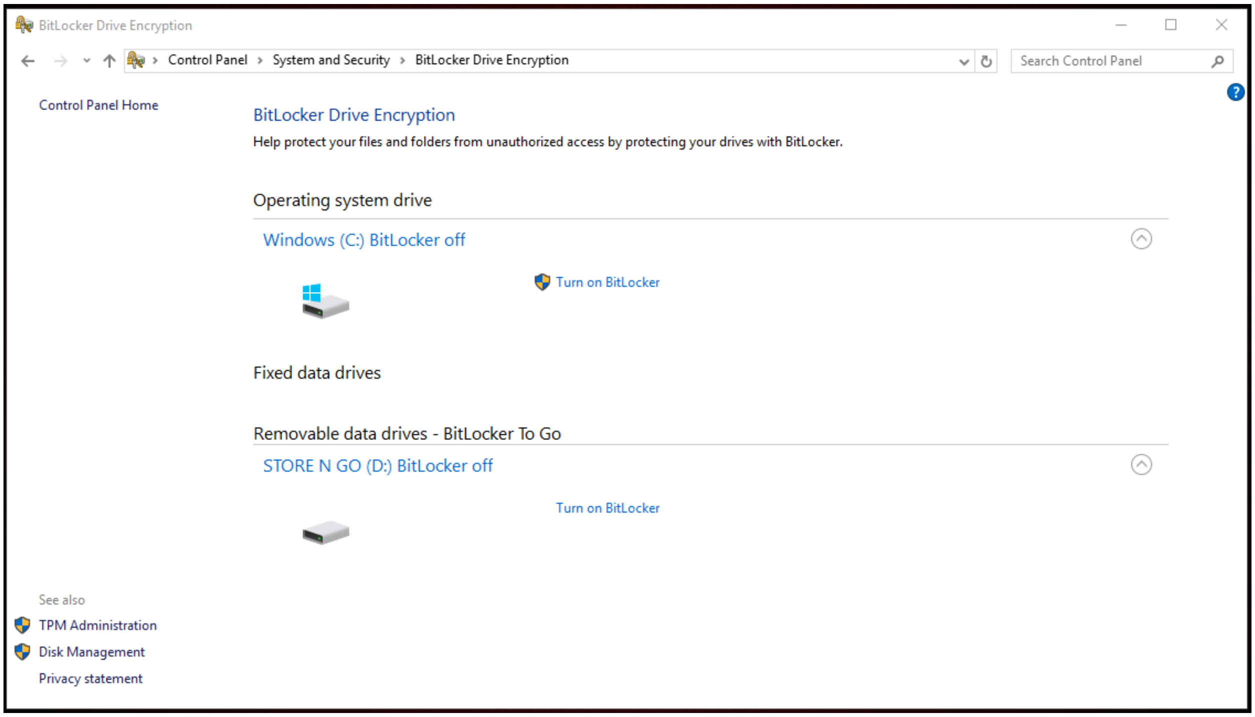
WARNING: Formatting will erase ALL data on this disk.
To format the disk, click OK. To quit, click CANCEL.

Once the format has completed you will see that the BitLocker is now off again.



Formatting STORE N GO (D:)

Format Complete.



BitLocker Drive Encryption

Control Panel > System and Security > BitLocker Drive Encryption

Search Control Panel

Control Panel Home

BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

Operating system drive

Windows (C:) BitLocker off

Turn on BitLocker

Fixed data drives

Removable data drives - BitLocker To Go

STORE N GO (D:) BitLocker off

Turn on BitLocker

See also

TPM Administration

Disk Management

Privacy statement

Step 3:

Now, to permanently destroy the encryption key, turn BitLocker back on.

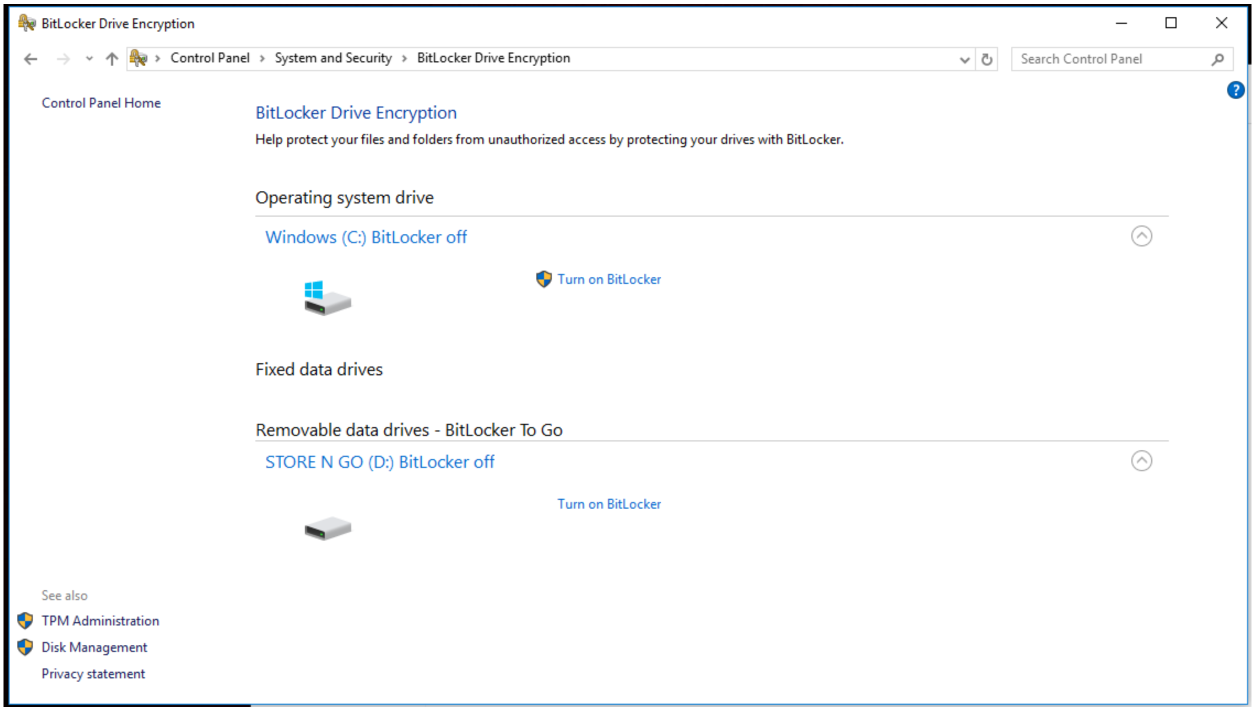
Go through the same steps we did previously.

- Set a unique password to unlock the device (pick a different password than you picked previously). Any random characters will suffice.
- Save or print the recovery key (then delete the file or shred the paper)
- You can choose to Encrypt only used space to speed up this second encryption process (we are really only interested in overwriting the encryption key).
- If you want to leave the drive encrypted, you will need to choose which encryption mode to use. If you are going to format the drive again after this process, it doesn't matter (this only applies to Windows 10).
- Start the encryption process (The encryption process should complete much faster this time).

Step 4:

Format the drive one more time. Again a quick format is fine.

At this point the drive has now been overwritten with encrypted data and the original encryption key has been destroyed. Any data on the drive is unrecoverable, random data. The drive can now be reused or redeployed as necessary.


BitLocker Drive Encryption
Control Panel > System and Security > BitLocker Drive Encryption
Search Control Panel
Control Panel Home

BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

Operating system drive

Windows (C:) BitLocker off

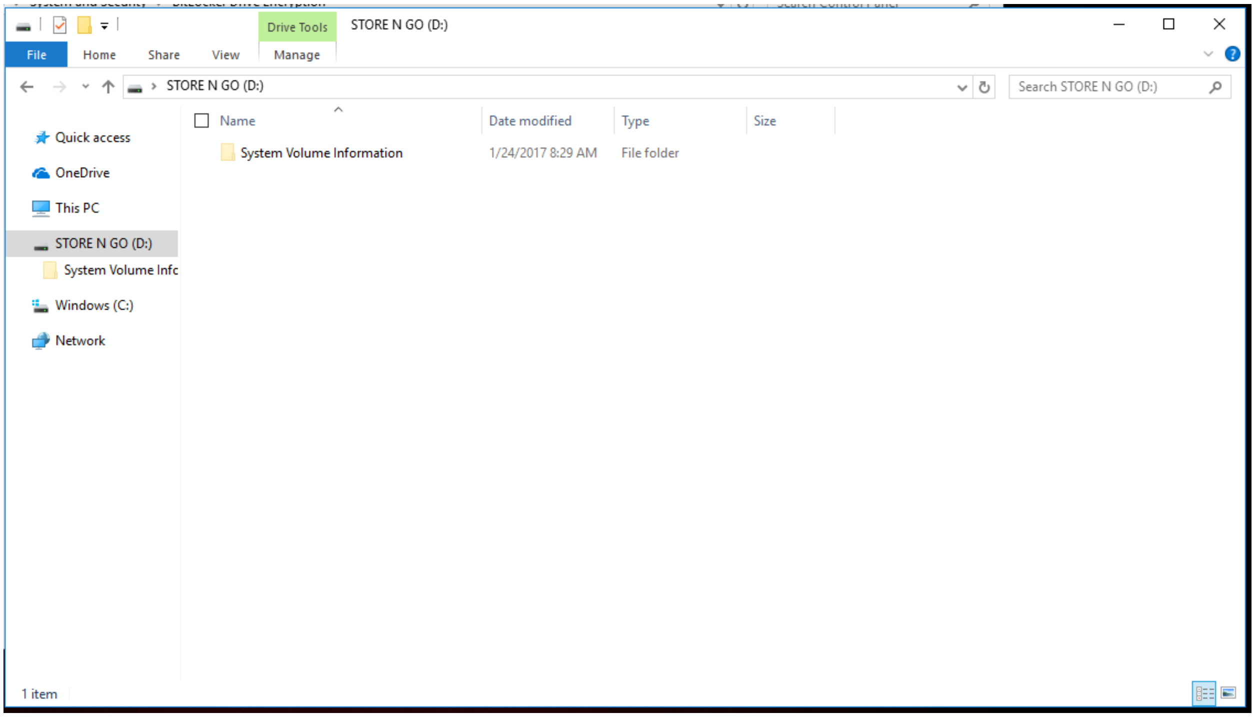
Turn on BitLocker

Fixed data drives

Removable data drives - BitLocker To Go

STORE N GO (D:) BitLocker off

Turn on BitLocker



Name	Date modified	Type	Size
System Volume Information	1/24/2017 8:29 AM	File folder	