Winaero

At the edge of tweaking

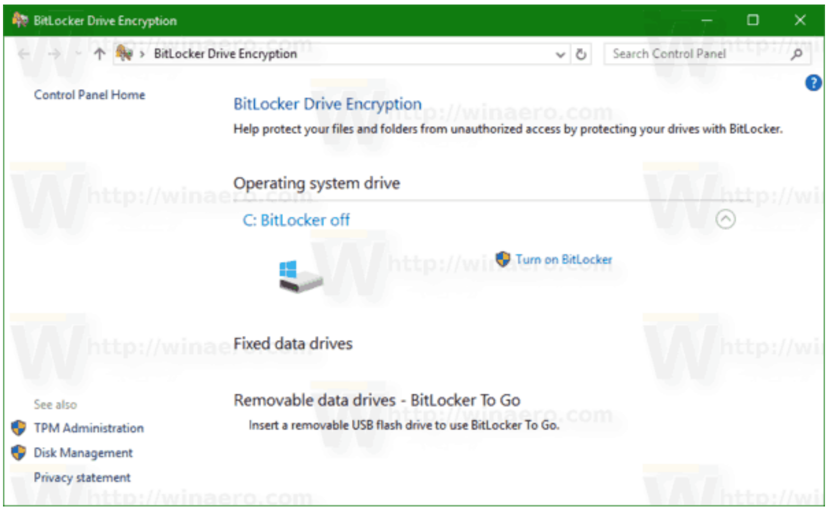
Turn On BitLocker for Fixed Drives in Windows 10

Turn On or Off BitLocker for Fixed Drives in Windows 10

For extra protection, Windows 10 allows enabling BitLocker for fixed drives (drive partitions and internal storage devices). It supports protection with a smart card or password. You can also make the drive to automatically unlock when you sign in to your user account.

RECOMMENDED: Click here to fix Windows errors and optimize system performance

BitLocker was first introduced in Windows Vista and still exists in Windows 10. It was implemented exclusively for Windows and has no official support in alternative operating systems. BitLocker can utilize your PC's Trusted Platform Module (TPM) to store its encryption key secrets. In modern versions of Windows such as Windows 8.1 and Windows 10, BitLocker supports hardware-accelerated encryption if certain requirements are met (the drive has to support it, Secure Boot must be on and many other requirements). Without hardware encryption, BitLocker switches to software-based encryption so there is a dip in your drive's performance. BitLocker in Windows 10 supports a number of encryption methods, and supports changing a cipher strength.



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

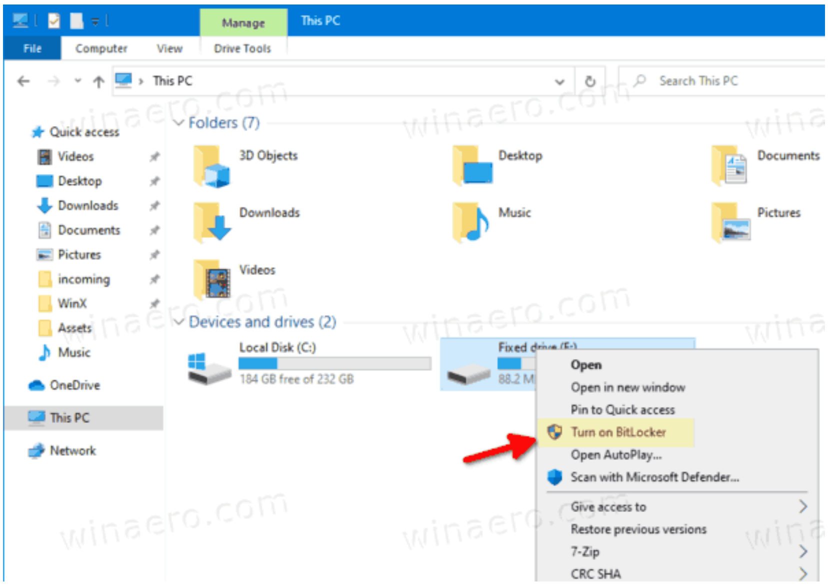
Insert a removable USB flash drive to use BitLocker To Go.

Note: In Windows 10, BitLocker Drive Encryption is only available in the Pro, Enterprise, and Education editions. BitLocker can encrypt the system drive (the drive Windows is installed on), and internal hard drives. The *BitLocker To Go* feature allows protecting files stored on a removable drives, such as a USB flash drive.

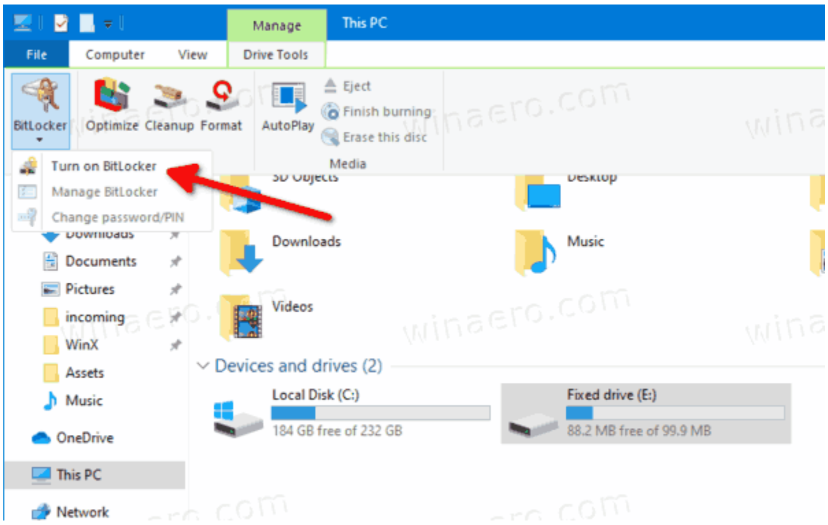
There are a number of methods you can use to turn on or off BitLocker for an internal fixed drive.

To Turn On BitLocker for a Fixed Data Drive in Windows 10,

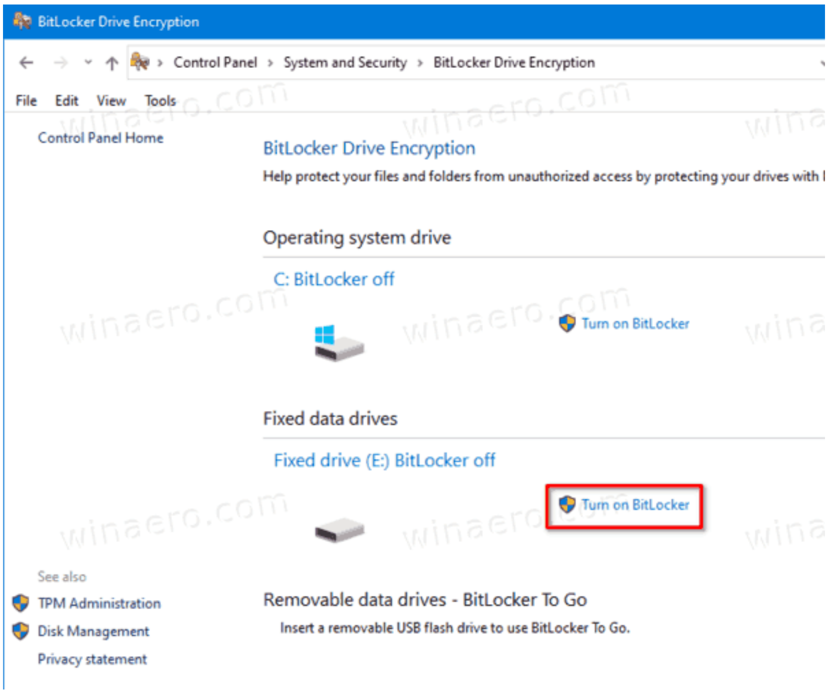
1. Configure the encryption method for BitLocker if required.
2. Open File Explorer to the This PC folder.
3. Right-click on the drive and select *Turn on Bitlocker* from the context menu.



4. Alternatively, click on *Manage* tab under *Drive Tools* in the Ribbon, then click on the *Turn on BitLocker* command.



5. Finally, you can open Control Panel\System and Security\BitLocker Drive Encryption. On the right, find your internal drive or partition, and click on the link *Turn on Bitlocker*.



BitLocker Drive Encryption

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

Operating system drive

C: BitLocker off

Turn on BitLocker

Fixed data drives

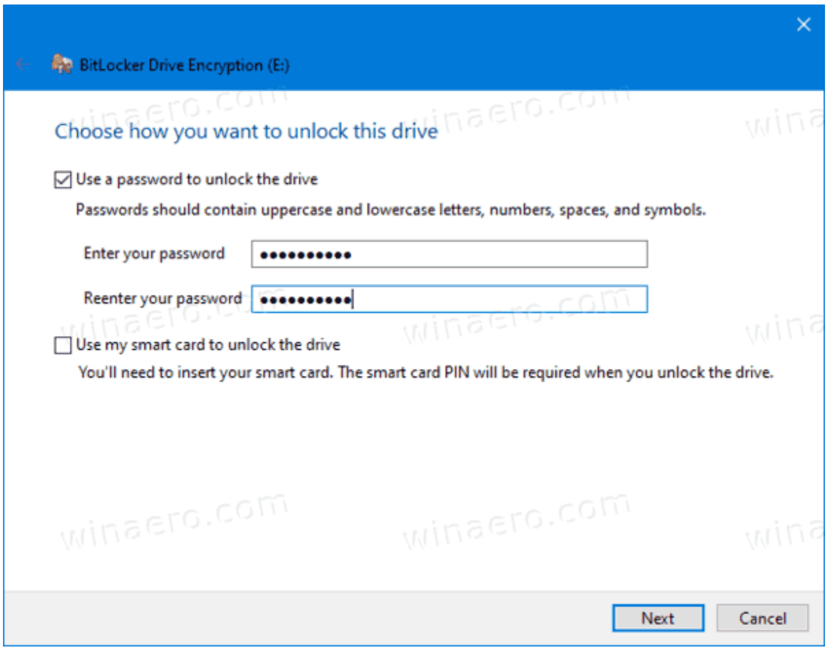
Fixed drive (E:) BitLocker off

Turn on BitLocker

Removable data drives - BitLocker To Go

Insert a removable USB flash drive to use BitLocker To Go.

6. In the next dialog, choose a smart card or provide a password to encrypt the drive contents.



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.

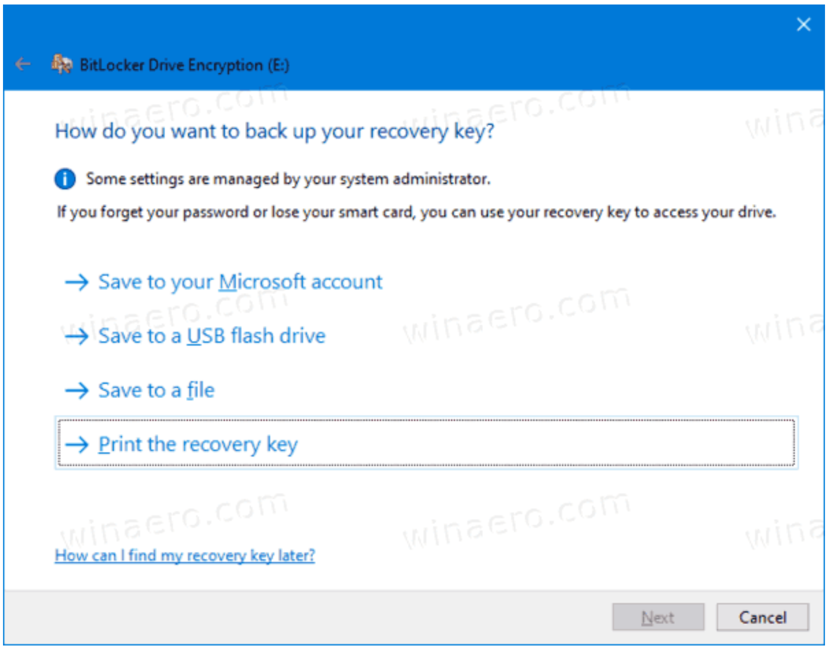
Enter your password ●●●●●●●●●●

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.

7. Choose how to backup the encryption key. For example, you can print it.



How do you want to back up your recovery key?

Some settings are managed by your system administrator.

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

→ Save to your Microsoft account

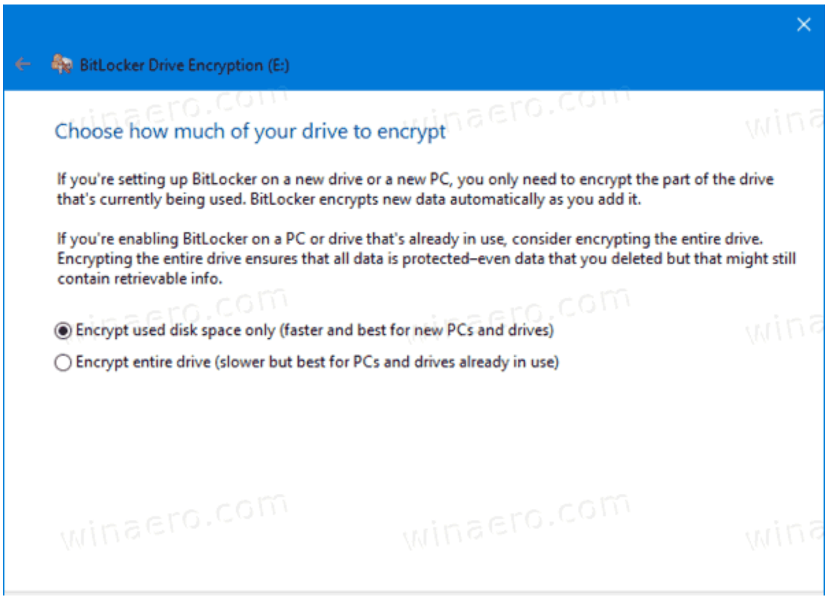
→ Save to a USB flash drive

→ Save to a file

→ Print the recovery key

How can I find my recovery key later?

8. Select how much of your drive space to encrypt. For new drives, you can choose 'used disk space only'. For drives that already contain files, choose *Encrypt entire drive*.



Choose how much of your drive to encrypt

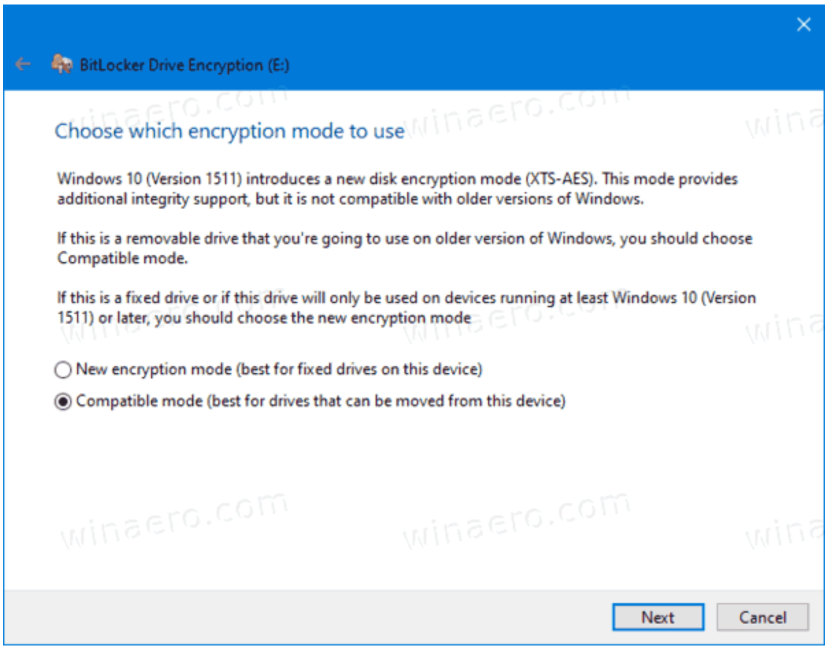
If you're setting up BitLocker on a new drive or a new PC, you only need to encrypt the part of the drive that's currently being used. BitLocker encrypts new data automatically as you add it.

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)

9. Specify which encryption mode to use.
    - *New encryption mode* (XTS-AES 128-bit) is supported on Windows 10.
    - *Compatible mode* (AES-CBC 128-bit) is supported on Windows Vista, Windows 7 and Windows 8/8.1.



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.

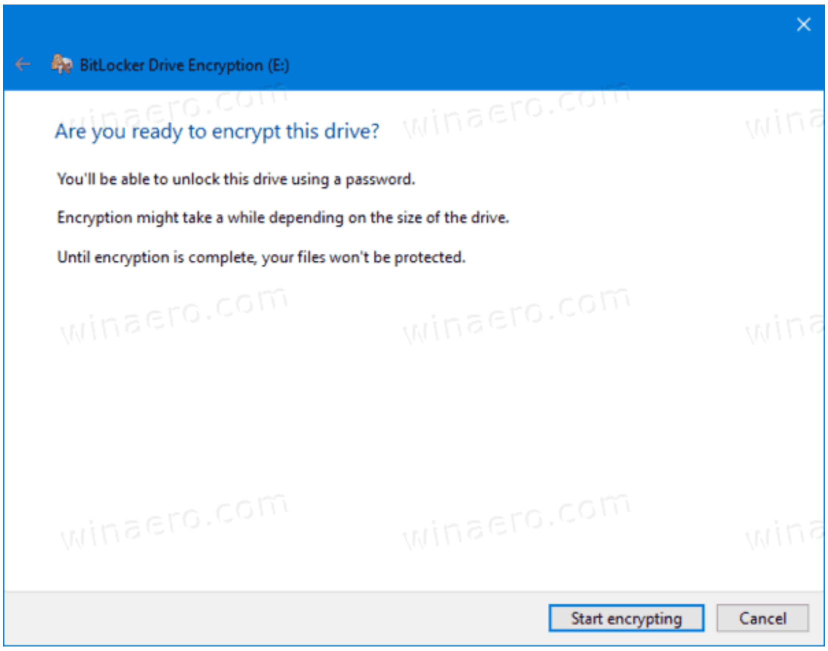
If this is a removable drive that you're going to use on older version of Windows, you should choose Compatible mode.

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)

10. Click on *Start encrypting*.



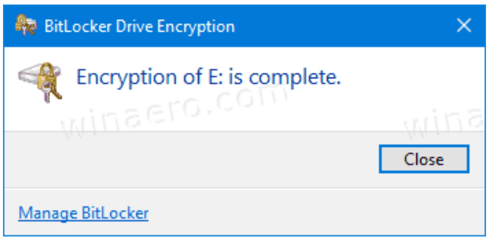
Are you ready to encrypt this drive?

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.

You are done. The fixed drive will be encrypted. This could take a long time to finish depending on the data size stored on the drive, and its capacity.

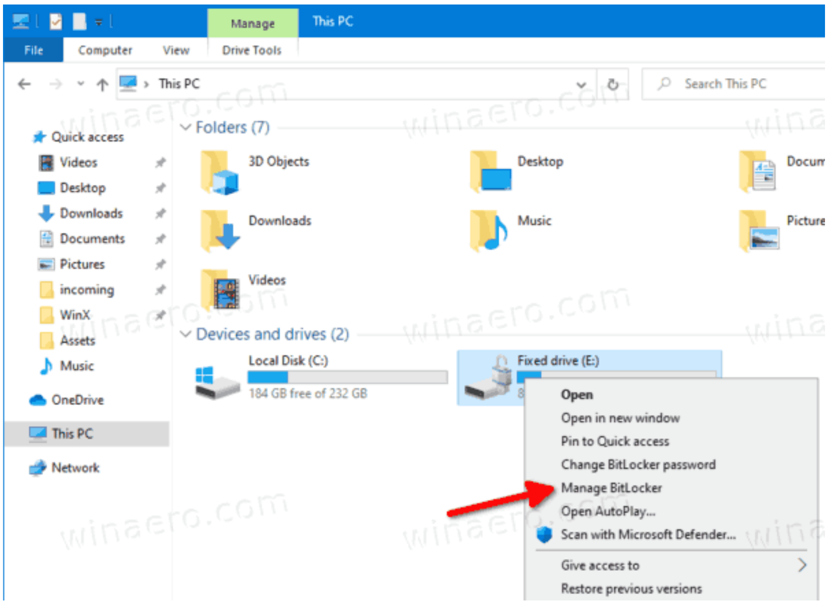


Encryption of E: is complete.

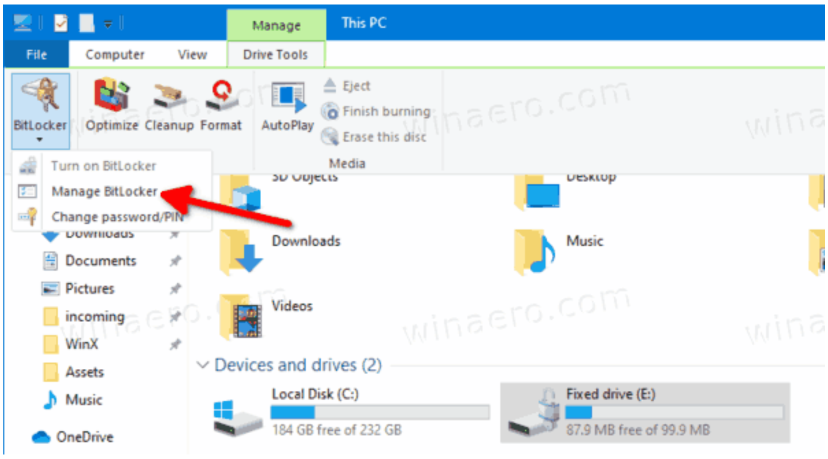
You can now check the BitLocker encryption status for the drive.

To Turn Off BitLocker for a Fixed Drive in Windows 10,

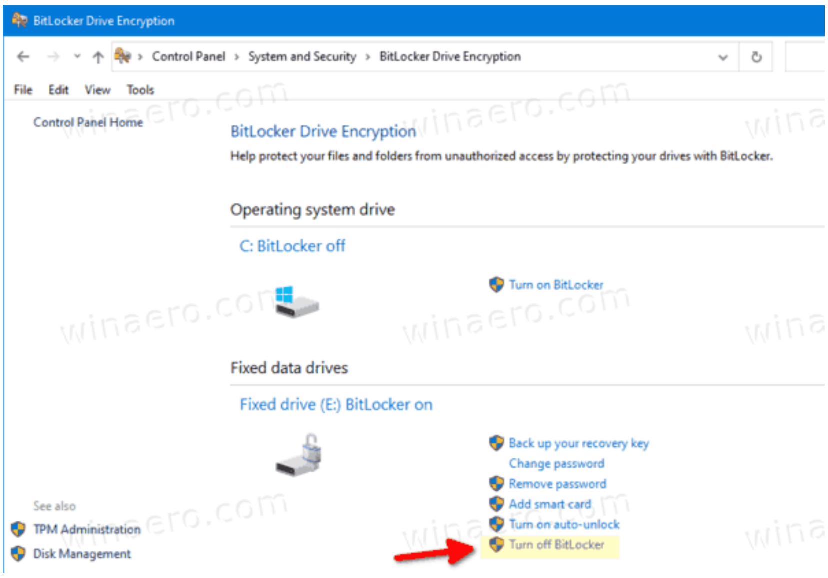
1. Open File Explorer to the This PC folder.
2. Right-click on the drive and select *Manage BitLocker* from the context menu.



3. Alternatively, click on *Manage* tab under *Drive Tools* in the Ribbon, then click on the *Manage BitLocker* command.



4. Finally, you can open Control Panel\System and Security\BitLocker Drive Encryption.
5. On the right side of the *Drive Encryption Dialog*, find your fixed drive, and click on the link *Turn off BitLocker*.



BitLocker Drive Encryption

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

Operating system drive

C: BitLocker off

Fixed data drives

Fixed drive (E:) BitLocker on

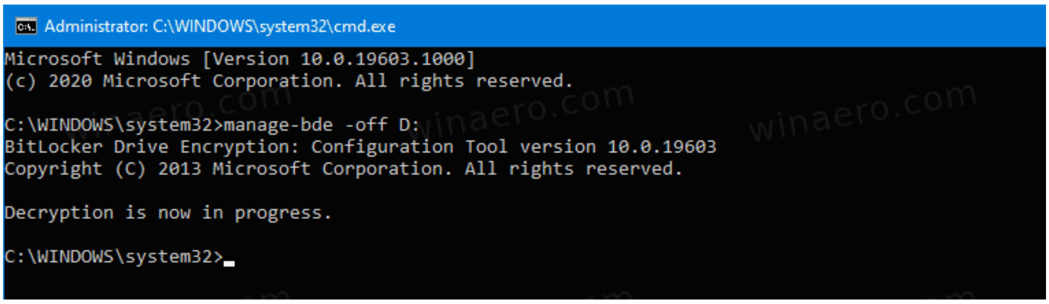
6. Click on the *Turn off BitLocker* to confirm the operation.

You are done. BitLocker will decrypting the drive contents.

You can now check the BitLocker encryption status for the drive.

Also, you can disable BitLocker for an internal drive from Command Prompt or PowerShell.

1. Open a new command prompt as Administrator.
2. Type and run the following command: `manage-bde -off <drive letter>:`.
3. Substitute `<drive letter>` with the actual drive letter of the drive you want to decrypt. For example: `manage-bde -off D:`.



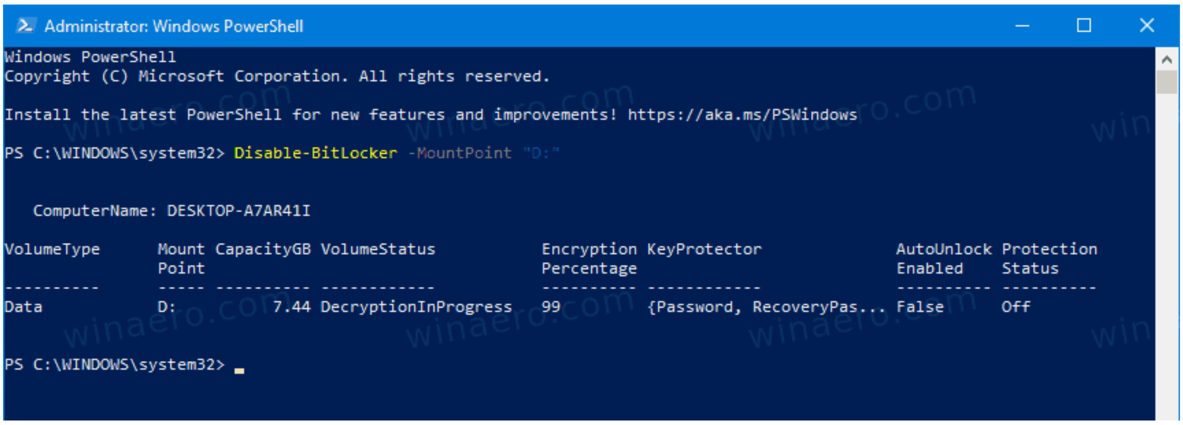
```
Microsoft Windows [Version 10.0.19603.1000]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>manage-bde -off D:
BitLocker Drive Encryption: Configuration Tool version 10.0.19603
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

Decryption is now in progress.

C:\WINDOWS\system32>_
```

4. Alternatively, open PowerShell as Administrator.
5. Type and run the following command: `Disable-BitLocker -MountPoint "<drive letter>:"`.
6. Substitute `<drive letter>` with the actual drive letter of the drive you want to decrypt. For example: `Disable-BitLocker -MountPoint "D:"`.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\WINDOWS\system32> Disable-BitLocker -MountPoint "D:"


   ComputerName: DESKTOP-A7AR41I

VolumeType      Mount CapacityGB VolumeStatus           Encryption KeyProtector              AutoUnlock Protection
                Point                                   Percentage                           Enabled    Status
----------      ----- ---------- ------------           ---------- ------------              ---------- ----------
Data            D:          7.44 DecryptionInProgress   99         {Password, RecoveryPas... False      Off

PS C:\WINDOWS\system32> _
```

You are done!

You can now check the BitLocker encryption status for the drive.

That's

You are here: Home » Windows 10 » Turn On BitLocker for Fixed Drives in Windows 10

Support us

Winaero greatly relies on your support. You can help the site keep bringing you interesting and useful content and software by using these options:

Donate

Bitcoin: 18amKj99FCPUfnnpqZ6XCG2h3TGeUTCeY7

Connect with us

For your convenience, you can subscribe to Winaero on the following web sites and services.

Follow 1,572 followers Telegram YouTube 999+

In addition, you can share this post.

Reddit Tweet Share Share

This entry was posted in Windows 10 and tagged Windows 10 Bitlocker on April 17, 2020 by Sergey Tkachenko.

About Sergey Tkachenko

Sergey Tkachenko is a software developer from Russia who started Winaero back in 2011. On this blog, Sergey is writing about everything connected to Microsoft, Windows and popular software. Follow him on Telegram, Twitter, and YouTube.

View all posts by Sergey Tkachenko →