BitLocker Drive Encryption

BitLocker, available on Windows 8.1 Pro and Windows 10, goes much farther than protecting individual files or folders; it can encrypt an entire drive. After all, when million-dollar corporate secrets are at stake, a determined, knowledgeable thief could swipe your laptop, nab your flash drive, or even steal the hard drive out of your desktop PC.

When you turn on this feature, your PC automatically encrypts (scrambles) everything on an *entire drive,* including all of Windows itself.

If the bad guy tries any industrial-strength tricks to get into the drive—trying to reprogram the startup routines, for example, or starting up from a different hard drive—BitLocker presents a steel-reinforced password screen. No password, no decryption.

You also get BitLocker to Go—a disk-encryption feature especially for removable drives like USB flash drives. Even if you lose it or leave it behind, it's worthless to anyone without the password.

You don't notice much difference when BitLocker is turned on. You log in as usual, clicking your name and typing your password. But if a malefactor ever gets his hands on the actual disk, he'll be in for a disappointing surprise.

BitLocker for a Hard Drive

Here's how to encrypt a hard drive (as opposed to a removable drive):

1. Open BitLocker Drive Encryption.

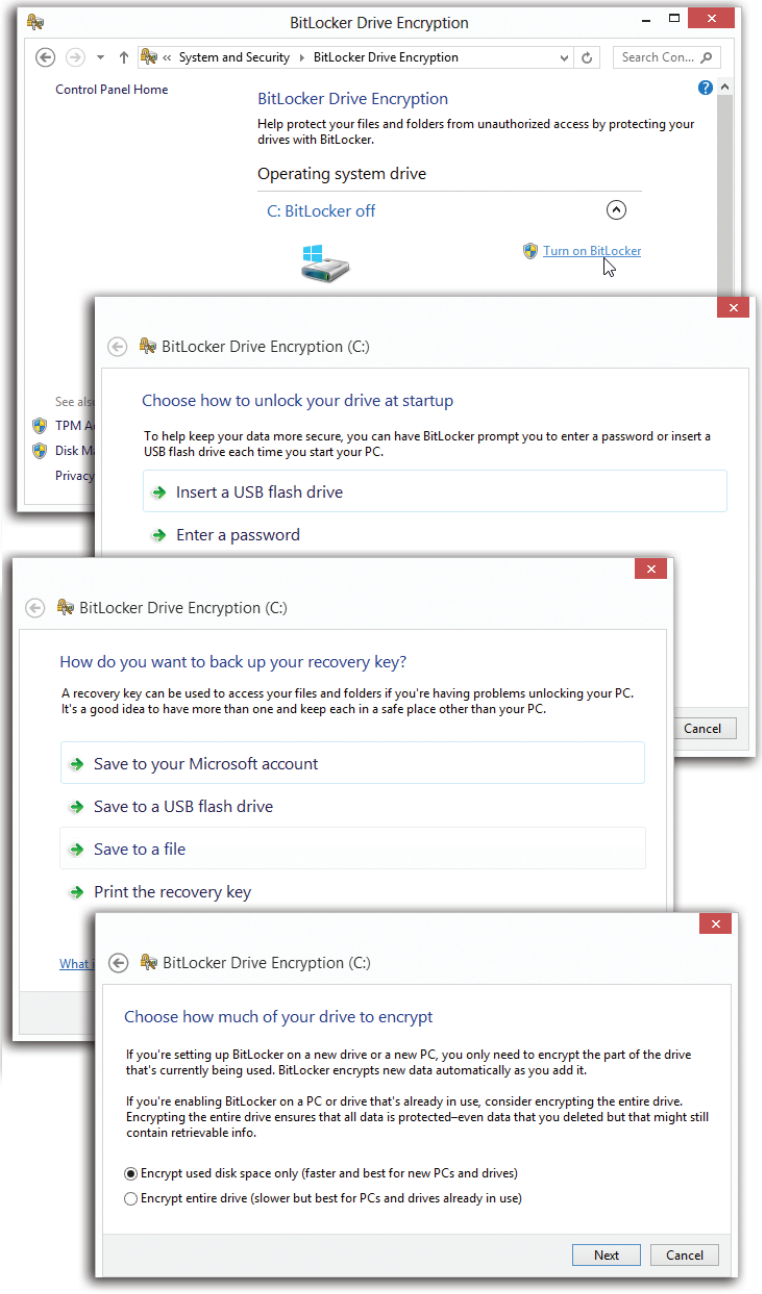

Figure 1:
Top: You get a separate "Turn On BitLocker" link for each drive listed in the Control Panel.

Second from top: Make up your primary password. It has to have capitals and lowercase letters, and numbers too. Or turn a flash drive into a physical key.

Third from top: Where do you want to store your last-ditch recovery key? Whatever you decide, don't lose the darned thing. You'll feel like an idiot if you attempt to stop a bad guy from getting to your files–and wind up stopping yourself *from getting to them because you lost the passwords.*

If you choose "to your Microsoft account," go here if you ever have to recover that key:

https://skydrive.live.com/RecoveryKey

Bottom: There's not much point to encrypting the empty space.

It's in your Control Panel, but the quickest way is probably to type *bitlock* into the Search box, and select **BitLocker Drive Encryption in the results.**

You see the display shown in Figure 1 at top, listing each of your disks. (Under a separate heading, you see the icons of removable disks like flash drives. For them, see "BitLocker to Go," below.)

2. **For the drive you want to protect, choose "Turn on BitLocker."**

   The message shown on the second screen in Figure 1 is asking what you want to use as your master key. Yes, you can make up a password. But you can also turn a USB flash drive into a physical key that can unlock your hard drive.

   Either way, don't mess around here. You're about to take the extraordinary step of encrypting your entire hard drive. If you lose that password or that flash drive, *all your files are gone forever.* Nothing can get them back.

3. **Click either "Insert a USB flash drive" or "Enter a password."**

   If you chose the flash-drive option, a window opens and shows you all the flash drives Windows can find. Click the one you want to use, and then click OK. Do not lose the flash drive.

   If you chose the password option, a window opens and asks you to enter a complex password. Twice. Do not forget it.

4. **Click Next.**

   Now you see the box shown in Figure 1 at bottom. Microsoft is giving you an out—a backup emergency recovery method—in case you lose your flash-drive "key" or forget the BitLocker password. It's allowing you to create a recovery key: a back door.

   The recovery key is a 48-digit serial number. You have four ways to save it: to your Microsoft account (that is, you're saving the key online); to *another* flash drive; to a file (hint: don't save it on the same computer you're protecting!); or as a printout.

Note: You can choose more than one of these options. You can save it *and* print it, for example. The dialog box doesn't go away until you click Next.

---

5. **Choose where to save the recovery-key number, and then click Next.**

   Now you see the box shown in Figure 1, bottom. Windows is offering to encrypt only the part of the disk that actually has files on it, which is much faster than encrypting the entire disk including empty space. Better yet, even if you choose "used disk space only," any new files you add later will be encrypted automatically.

6. **Click Next.**

Windows asks if you're ready to begin, and warns you that the PC might feel sluggish while the encryption is going on. (This can take some time.)

7. **Click Continue and then "Restart now."**

   The computer restarts.

From now on, every time you turn on the computer (or, more specifically, every time Windows tries to access the encrypted drive, you have to supply your BitLocker password (or insert the flash drive "key").

If you don't have the password or flash drive (gulp), press the Esc key to use the recovery key from step 4. That's your last chance.

Tip: For drives *other* than your Windows drive, you can turn on "Automatically unlock," which saves you that additional password-entering business; see page 5.)

Otherwise, you won't notice any difference in your usual routine. But, of course, something is different: You're now protected, even from the most determined and knowledgeable hard drive thieves.

BitLocker to Go

Windows also offers a feature just for removable drives (mainly USB flash drives): BitLocker to Go. It works the same way—you create a password and a backup password (recovery key), and then Windows encrypts the drive—but it's arguably even more useful, because removable drives are portable. It's understood that you'll be taking it out into the big dangerous world. You're much more likely to lose a flash drive than to be the victim of a midnight hard drive–removal raid.

The steps go like this:

1. **Open the Control Panel, and select System & Security→BitLocker Drive Encryption.**

   You see the display shown in Figure 1 at top, listing each of your disks.

2. **Under "Removable data drives —BitLocker to Go," find the icon of the drive you want to encrypt. Click "Turn On BitLocker" next to it.**

   After a moment, you get the message shown in Figure 2. It's asking whether you want to use a password as the unlocking key, or a smart card that's been issued to you by your corporate network geek.

3. **Make your selection.**

   If you choose the password option, you're now asked to make up a hard-to-crack one. Enter it twice.

   If you chose the smart card option, insert the card into your computer's reader.

4. **Click Next.**

   Now you see a box like the one in Figure 5, third from top. Here again, Microsoft is helping you create a backup key, in case you forget the BitLocker password. It's a 48-digit serial number. You have three ways to save it: to your Microsoft account (that is, you're saving the key online); to a file on the computer; or as a printout.

Figure 23-7: *You don't need that mysterious Trusted Computing Module chip when you're trying to BitLocker a flash drive, thank goodness.*

The decision you have to make here is easy: Use the "smart card" option only if you work in a corporation where somebody gave you a smart card to use.

Note: A reminder: You can choose more than one of these options.

5. **Choose where to save the recovery-key number, and then click Next.**

   Now Windows wants to know if it should encrypt only the part of the disk that actually has files on it (theoretically faster), or the entire drive. For a flash drive, there's not much difference in speed.

6. **Make your selection and click Next.**

   Windows warns you that the PC might feel slow while the encryption is going on.

7. **Click "Start encryption."**

   That's it. Once your flash drive is encrypted, you'll be asked for its key when you insert it into any Windows computer.

BitLocker Options

Once you've turned on BitLocker for a drive—any drive—the same Control Panel panel that began your adventure now shows a list of useful commands next to the drive's icon. You can change the password, remove the password, turn off BitLocker, and so on. After all, you probably won't work for the CIA forever.

One of the most useful is "Turn on auto-unlock." It means that, yes, you won't have to enter your BitLocker password for the corresponding drive every darned time you

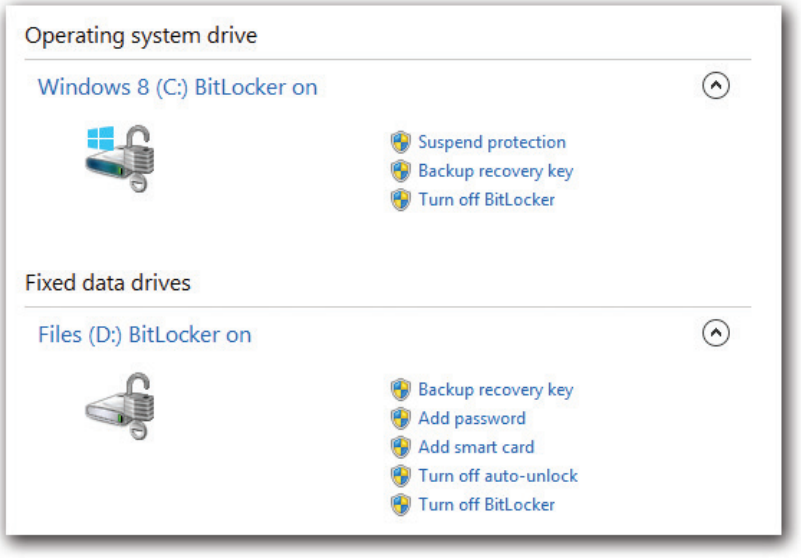

Figure 3: *After BitLocker is turned on, the main Windows drive (top) and other drives (bottom) offer different options. "Auto-unlock" is available only for your non-startup drives.*

turn on the PC. As you can see in Figure 3, it's available for any drive *except* the one you're running Windows from.