Widener University
Commonwealth Law School

Information Technology Services
Harrisburg Client Experience

BitLocker is a feature of Windows that encrypts your data to keep it safe from unauthorized access. Using BitLocker Whole Disk Encryption (WDE), your entire hard drive is encrypted. BitLocker is one very effective part of an overall protection strategy. Although it does not prevent hardware problems, malware, or accidental deletion of files, BitLocker will prevent an unauthorized person from gaining access to the data that is stored on your computer. That is very important to Widener University’s reputation and legal standing. Information Technology Services requires full-disk encryption for all University-owned desktops, laptops, and other portable computing devices.

What is encryption?

Encryption is the process of scrambling data to make it unreadable to anyone who does not possess the proper key. When you encrypt an entire hard drive using BitLocker, all of the files on the computer are encrypted.

When you log on to an encrypted computer, your hard drive is decrypted. When you shut down your system, the hard drive is re-encrypted. This means that when your device is powered off, your hard drive is protected against use by others.

Remember that once you unlock a hard drive, its files are available to you AND anyone else who can physically use your system. If you leave your system unattended, your files are not encrypted.

Is BitLocker available for Mac computers?

Because BitLocker is a component of the Microsoft Windows operating system, it is not available for Macs. For Macs, use FileVault instead.

Where is the BitLocker “key” stored?

BitLocker stores your recovery key in your computer's object in Active Directory. This means your key will be stored centrally, backed up regularly, and kept safe in case you need it later.

Will my computer have problems reading the encrypted disk if my computer is not connected to the network?

No, Active Directory is used to store your BitLocker recovery key. That is not needed for normal operation of your computer. The key is only in case something goes wrong and you need to recover the har drive with a technician's help.

What could go wrong?

If the part of your hard drive that starts up your computer (known as the boot loader) becomes corrupt, Windows may not be able to read your encrypted disk without the recovery key. Certain viruses and other malware can cause this, as can physical damage. If you move an encrypted drive from one computer to another, Windows will require your recovery key in order to read the drive. This is why it's important to store your BitLocker recovery key in the domain. If you need to enter Windows Safe Mode to uninstall software, run an anti-virus product, or repair your drive, BitLocker will again prompt for your recovery key.

Won't it slow my computer down?

No, there should be no noticeable effect on system performance at all. Microsoft says BitLocker adds approximately 1% overhead. If you have an older or lower-end system, please reach out to Client Experience to discuss options.

I'm told that BitLocker requires a TPM 1.2 chip. How can I find out whether I have one?

The Client Experience Team will determine if your computer meets Microsoft’s specifications. If it doesn’t, they will discuss alternatives with you.

My computer does not meet the specifications. Do I have to replace it?

No, not immediately. When your computer reaches the end of its usable life, it will be replaced during Asset Management with a computer that meets the requirements for BitLocker.

I have a Macintosh or Linux-based computer. What do I do?

Options exist for Macintosh and Linux-based computers, but some are still under development and they may be complex depending on what is installed on the computer. Talk to your Client Experience Team to determine the best option for your needs.

How long will it take?

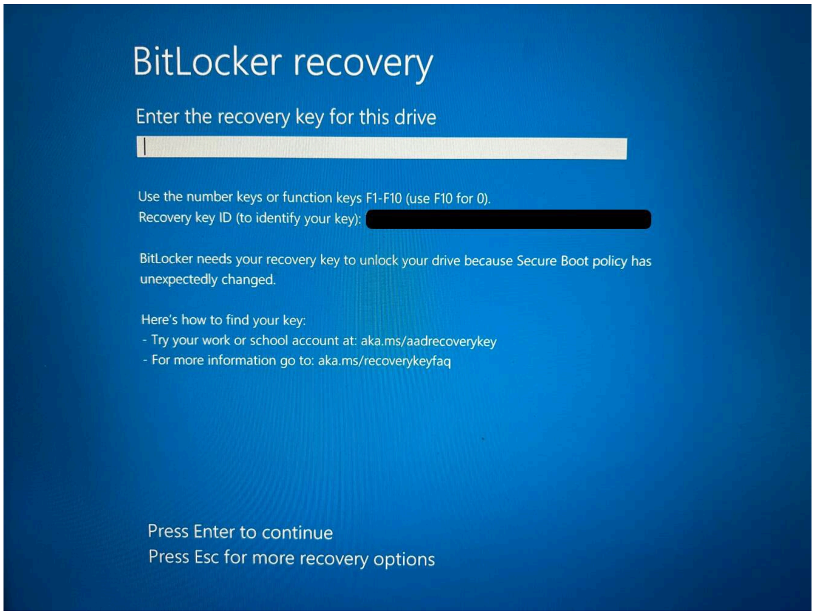
Typically, two to four hours. Make sure the computer is plugged in. You can continue to use your computer while BitLocker is encrypting the hard drive.

Yikes! BitLocker is encrypting my hard drive and suddenly I have no disk space free. Is it going to fill up my drive completely?

No. During the encryption process, your drive will appear to be nearly full. This is normal, but your usage will drop back down to its previous level once the encryption process is complete.

Yikes! My computer is "bricked." What now?

If you see a screen similar to this, contact the Helpdesk or the Client Experience Team for your campus. You will be asked for the Recovery Key ID and they will provide the recovery key for your computer.



BitLocker recovery

Enter the recovery key for this drive

Use the number keys or function keys F1-F10 (use F10 for 0).
Recovery key ID (to identify your key): [redacted]

BitLocker needs your recovery key to unlock your drive because Secure Boot policy has unexpectedly changed.

Here's how to find your key:
- Try your work or school account at: aka.ms/aadrecoverykey
- For more information go to: aka.ms/recoverykeyfaq

Press Enter to continue
Press Esc for more recovery options

My computer is lost or stolen! What now?

Report it as you normally would, but make sure to report that the computer was using whole disk encryption (assuming you had BitLocker running on it). And be happy that you protected critical information from compromise, prevented identities from being stolen, and helped to keep Widener's good reputation intact!