



Anywhere  
OPSWAT Guide



## INTRODUCTION

OPSWAT - cybersecurity solutions to identify, detect, and remediate advanced security threats from data and devices coming into and out of enterprise networks.

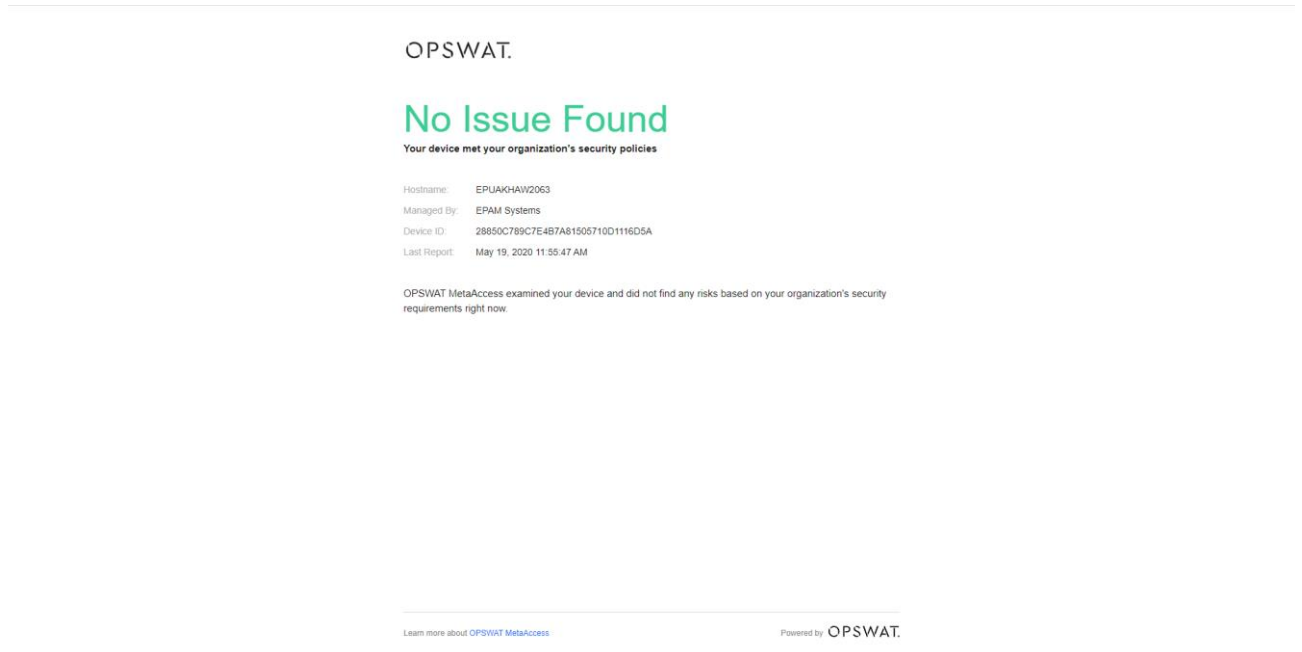
Here's what you need to do to be compliant with EPAM OPSWAT practices:

# CONTENTS

- OPSWAT ISSUES .....4
- BASIC OPSWAT CHECKS .....6
- 1. Encryption Disk for Windows .....6
- 2. Encryption Disk for MacOS .....15
- 3. Firewall for MacOS .....17
- 4. Antivirus programs .....18
- STILL NEED HELP? .....18

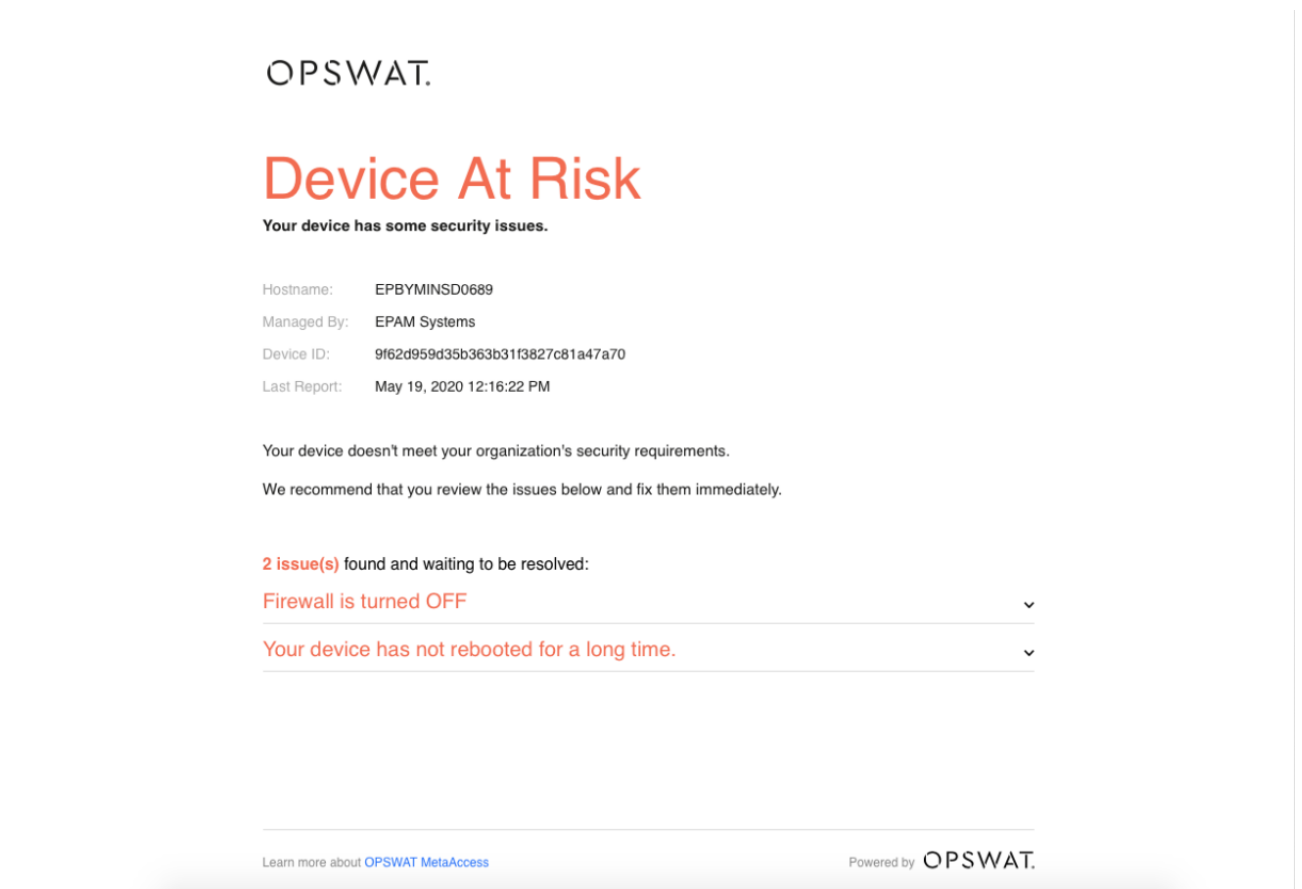
# OPSWAT ISSUES

OPSWAT client a tool that improves the security of your computers, checks processes, and files for threats, reliably protects access to data. In the presence of threats, the OPSWAT Client does not allow access to corporate sites. To see the status, click on the OPSWAT Client icon, after which you will go to the OPSWAT page with all the information.



The screenshot shows the OPSWAT interface with a green header 'OPSWAT.' and a large green title 'No Issue Found'. Below the title, it states 'Your device met your organization's security policies'. A metadata section lists: Hostname: EPJAKHAW2063, Managed By: EPAM Systems, Device ID: 28850C789C7E4B7A81505710D116D5A, and Last Report: May 19, 2020 11:55:47 AM. A footer note says 'OPSWAT MetaAccess examined your device and did not find any risks based on your organization's security requirements right now.' At the bottom, there are links for 'Learn more about OPSWAT MetaAccess' and 'Powered by OPSWAT.'

If your device has any issues, you will see a page with a list of errors.



The screenshot shows the OPSWAT interface with a red header 'OPSWAT.' and a large red title 'Device At Risk'. Below the title, it states 'Your device has some security issues.' A metadata section lists: Hostname: EPBYMINS0689, Managed By: EPAM Systems, Device ID: 9f62d959d35b363b31f3827c81a47a70, and Last Report: May 19, 2020 12:16:22 PM. A warning message says 'Your device doesn't meet your organization's security requirements. We recommend that you review the issues below and fix them immediately.' Below this, it says '2 issue(s) found and waiting to be resolved:' followed by two expandable items: 'Firewall is turned OFF' and 'Your device has not rebooted for a long time.' At the bottom, there are links for 'Learn more about OPSWAT MetaAccess' and 'Powered by OPSWAT.'

For a detailed description of the issue and its correction, expand it by clicking on it.

2 issue(s) found and waiting to be resolved:

### Firewall is turned OFF

#### What went wrong?

None of your firewall is ON

- Mac OS X Builtin Firewall

#### Why does it matter?

A properly configured firewall helps to keep attackers, external threats, or malicious internet traffic from getting access to your device.

#### How do I fix this?

Please [click here](#) to learn how to turn on firewall on your device.

### Your device has not rebooted for a long time.

#### What went wrong?

Your device has not rebooted for a long time.

#### Why does it matter?

Rebooting your system frequently helps your computer work more efficiently.

#### How do I fix this?

Please reboot your system as soon as possible.

'How do I fix this' describes what needs to be done to fix the issue. In most cases, this section offers to follow the 'click here' link for a detailed step by step guide.

The screenshot shows a web browser window with the URL [onlinehelp.opswat.com](https://onlinehelp.opswat.com). The page title is "Firewall Remediation Instruction - MetaAccess". The main content area is titled "Firewall Remediation Instruction" and includes the following text:

Steps to turn on Firewall on your devices:

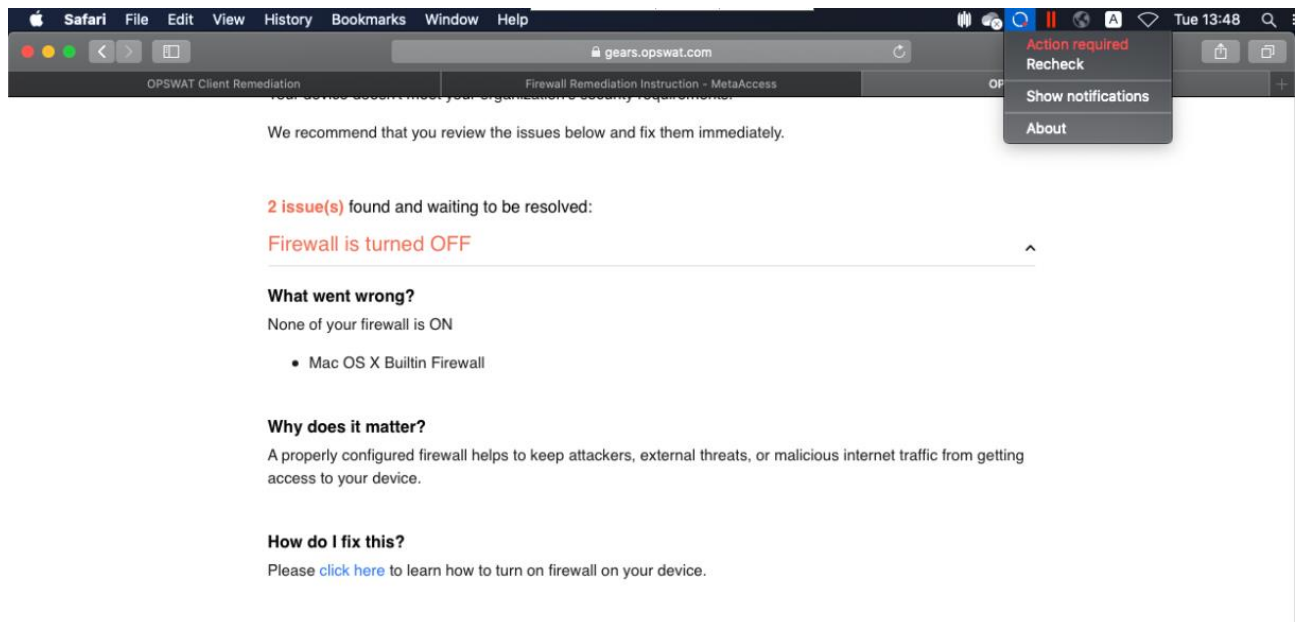
1. Turn on firewall at least on one of your firewall products: follow guideline from your organization or Firewall vendor to turn firewall on. Below are some references
  - a. [Windows Defender Firewall](#)
  - b. [Mac OS X Firewall](#)
2. Click on OPSWAT Client tray icon, select "Recheck" or "Check applications security" depends on the agent version you are running. Wait few minutes and check again.

A screenshot of the OPSWAT Client tray icon is shown, with a red box highlighting the "Recheck" button. The tray icon also shows "Show Notifications" (checked) and "About".

If you already turn on Firewall but the issue still occurs, please log into [OPSWAT Portal](#) and open a support ticket with us. Please attach screenshots which proves that Firewall status is ON and version of the product installed to the ticket.

Navigation links at the bottom include: < BitLocker Drive Encryption - Encryption ... and User Authentication Issues >

After fixing the problem, click the OPSWAT client icon and do 'Recheck' to apply fixes.



## BASIC OPSWAT CHECKS

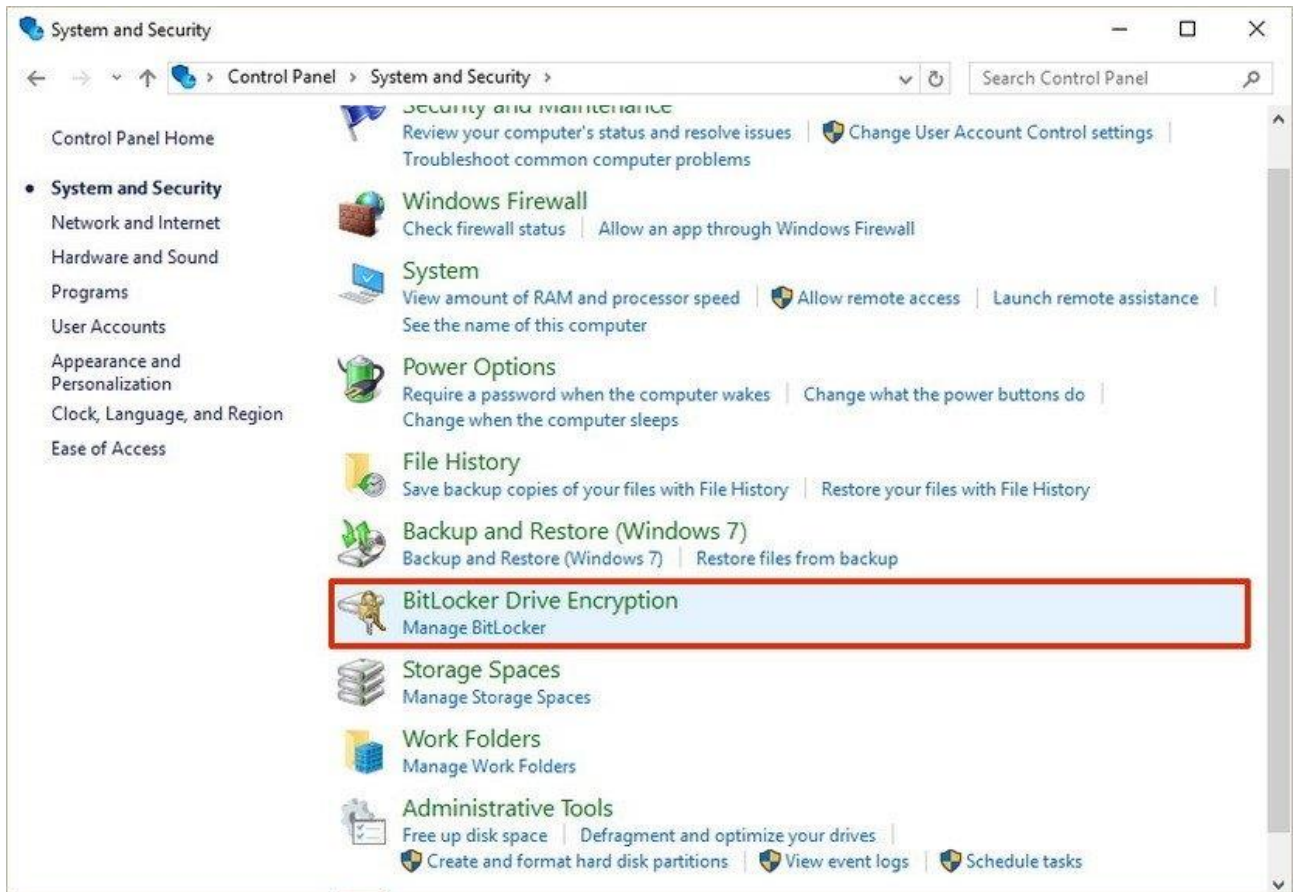
### 1. Encryption Disk for Windows

OPSWAT checks your computer for encrypted disks.

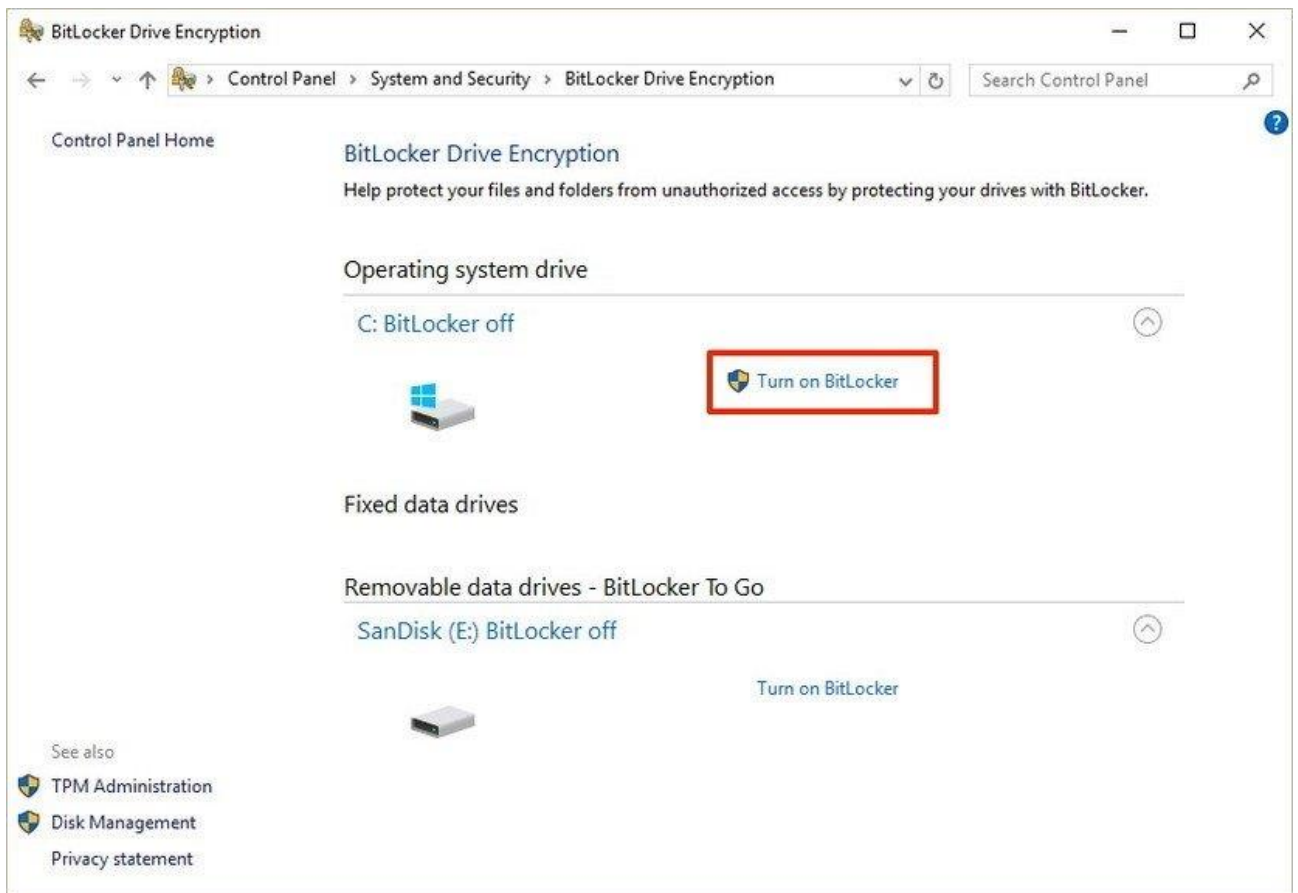
For Windows operating systems (**Pro, Enterprise, and Education**) Bitlocker is a preinstalled application that performs disk encryption.

For Enable Bitlocker on Windows (**Pro, Enterprise, and Education**).

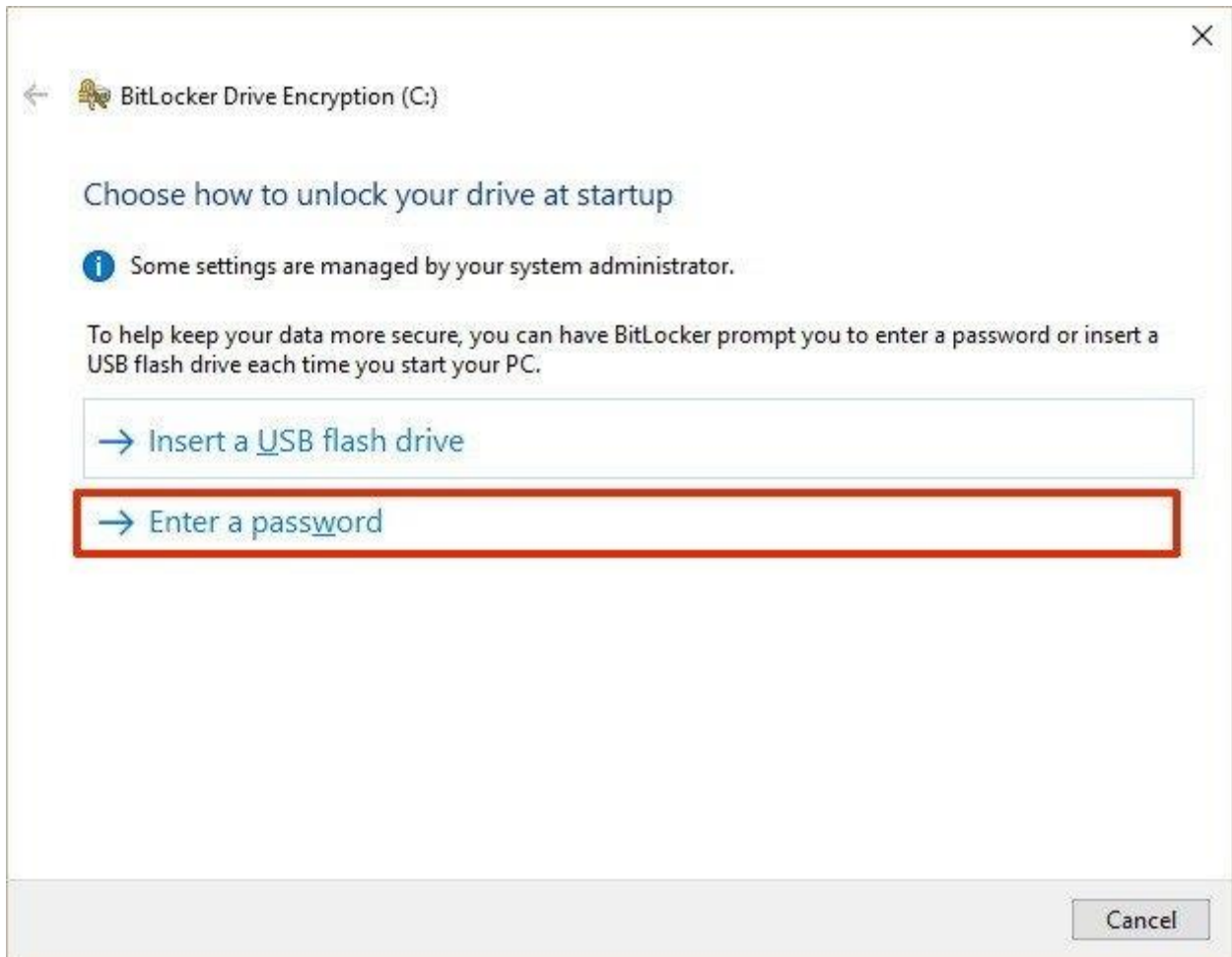
1. Use the **Windows key + X** keyboard shortcut to open the Power User menu and select **Control Panel**.
2. Click **System and Security**.
3. Click **BitLocker Drive Encryption**.



4. Under BitLocker Drive Encryption, click **Turn on BitLocker**.

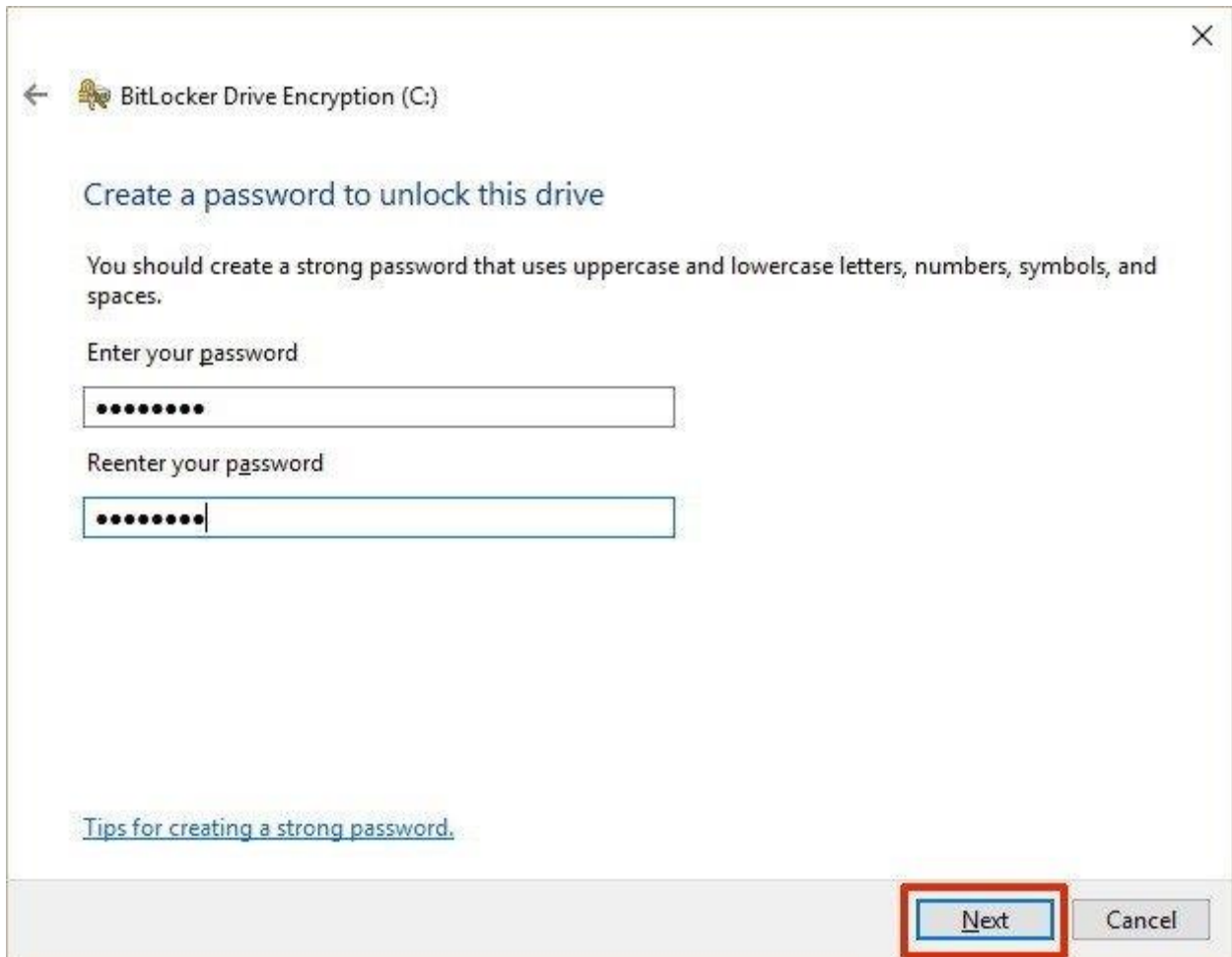


5. Choose how you want to unlock your drive during startup: **Insert a USB flash drive** or **Enter a password**. For the purpose of the guide, select **Enter a password** to continue.

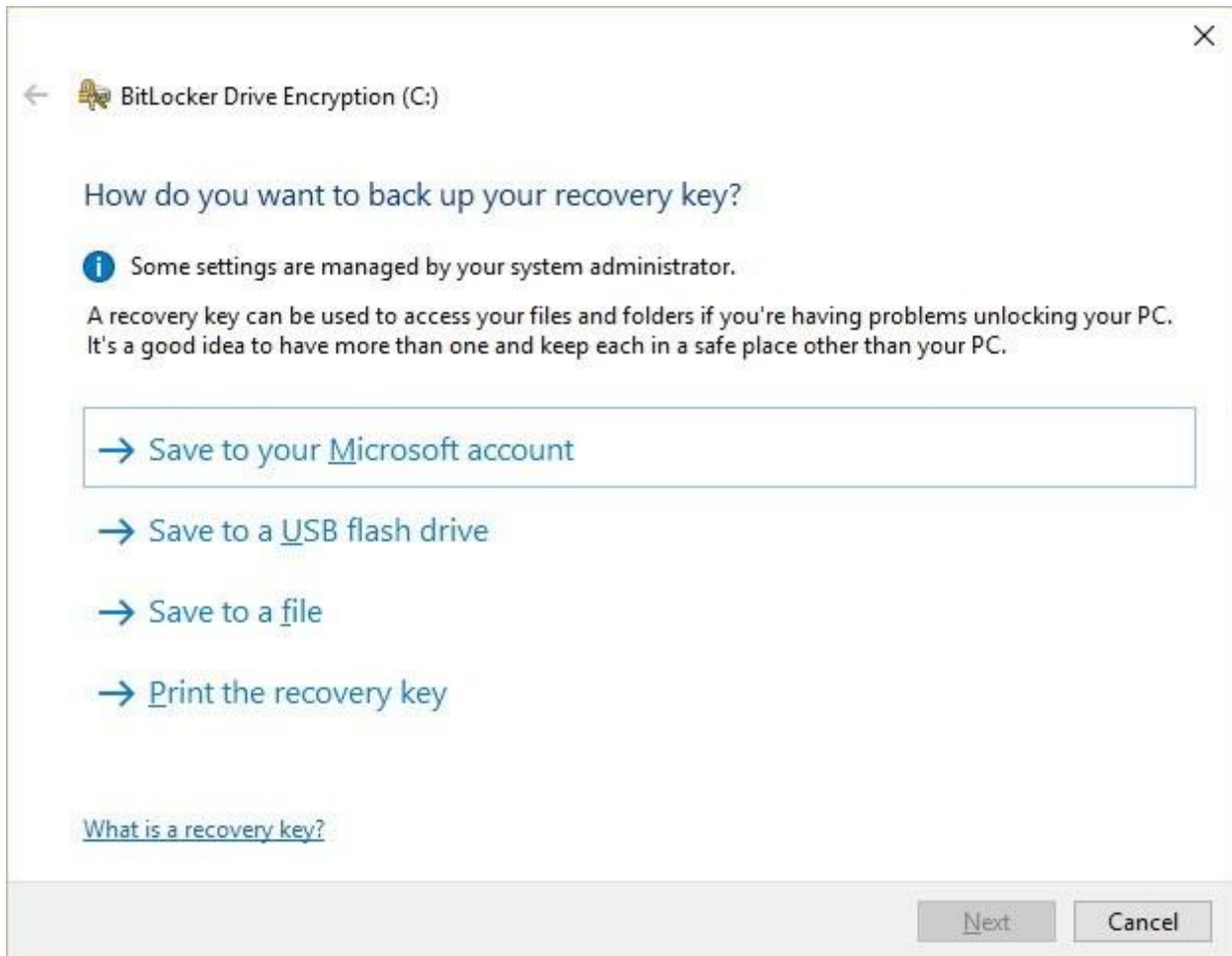


6. Enter a password that you'll use every time you boot Windows 10 to unlock the drive and click **Next** to continue. (Make sure to create a strong password mixing uppercase, lowercase, numbers, and symbols.)





7. You will be given the choices to save a recovery key to regain access to your files in case you forget your password. Options include:
  - Save to your Microsoft account;
  - Save to a USB flash drive;
  - Save to a file;
  - Print the recovery.Select the option that is most convenient for you and save the recovery key in a safe place.
8. Click **Next** to continue.



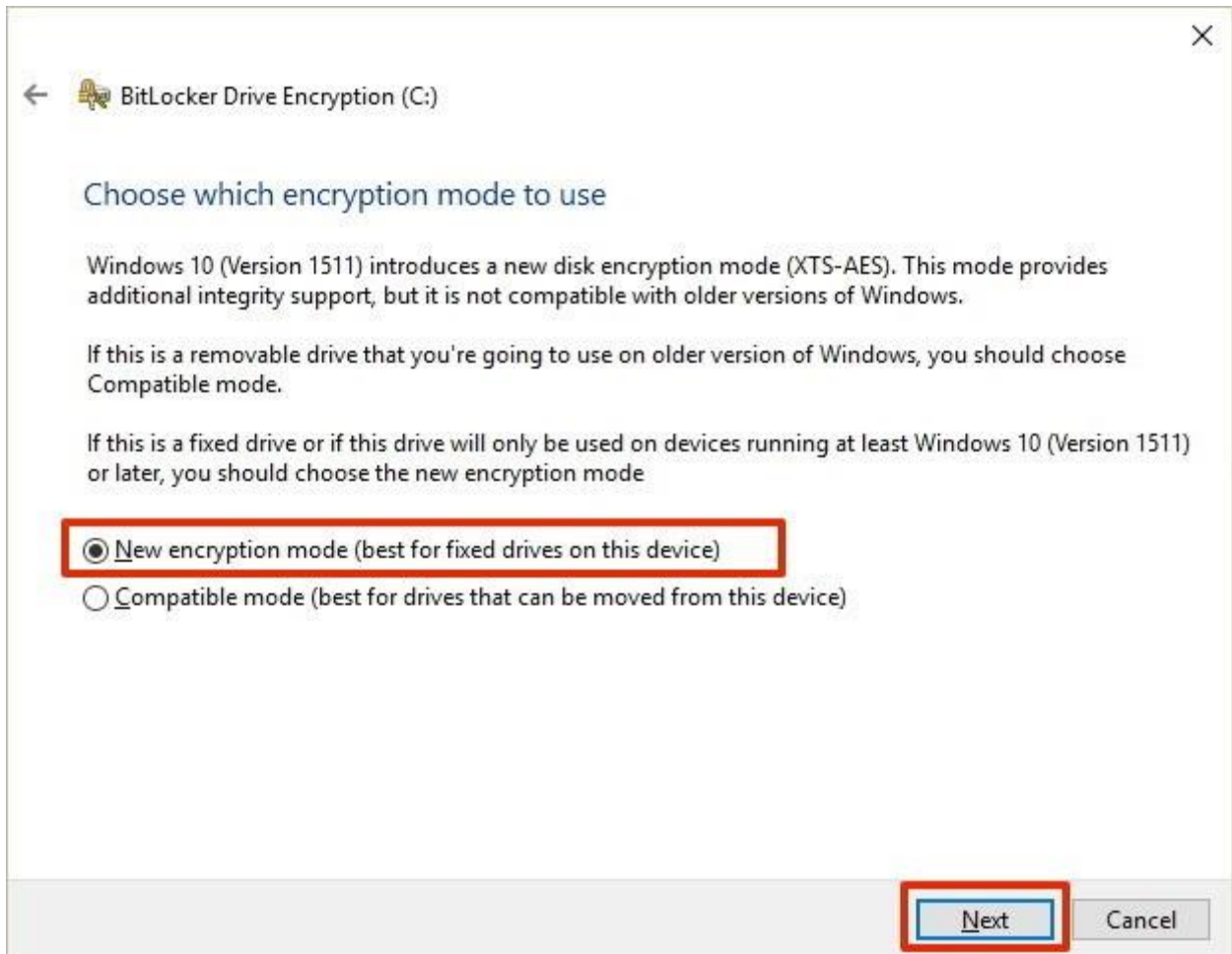
9. Select the encryption option that best suits your scenario:

- 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)

10. Choose between the two encryption options:

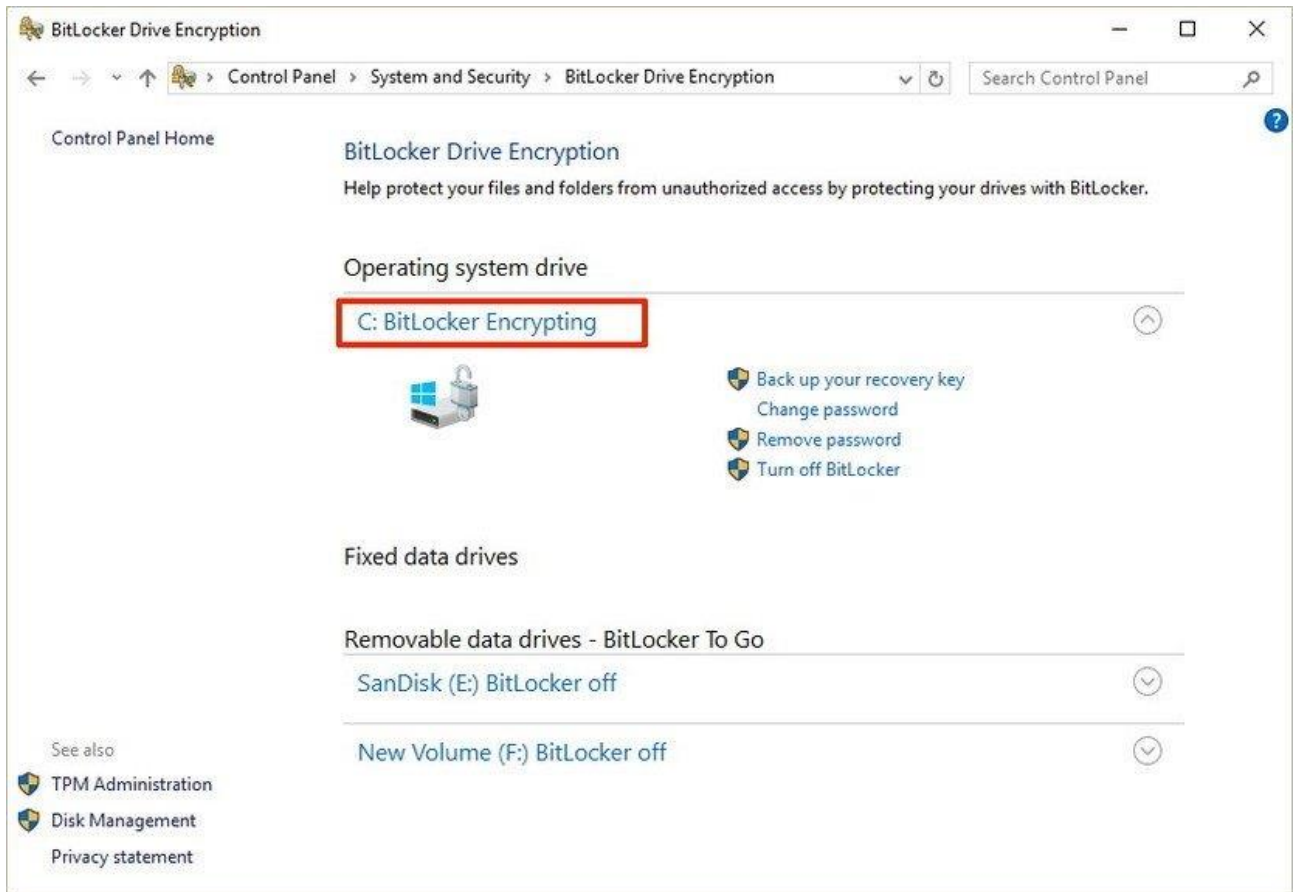
- New encryption mode (best for fixed drives on this device)
- Compatible mode (best for drives that can be moved from this device)

11. Click **Next** to continue.

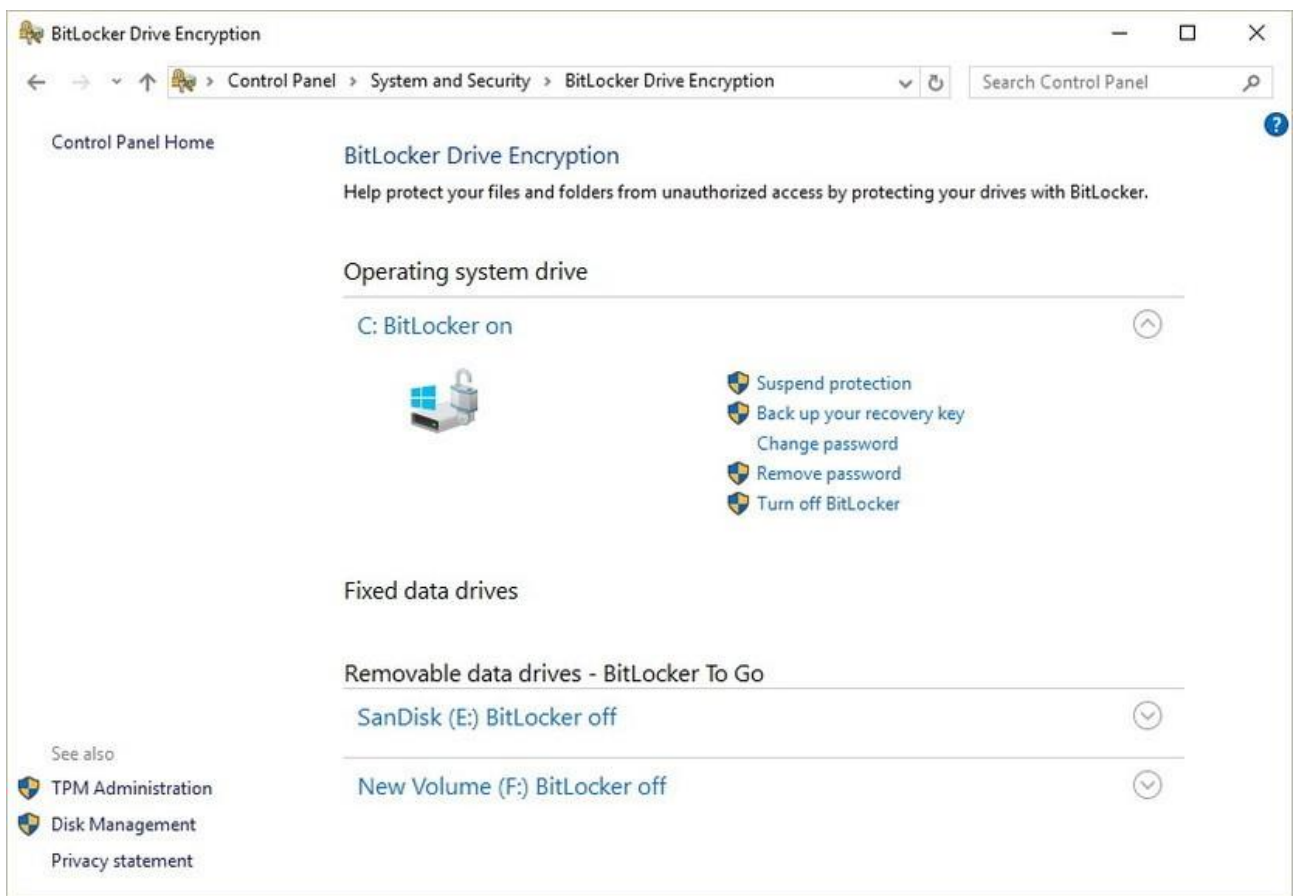


12. Finally, restart your computer to begin the encryption process.

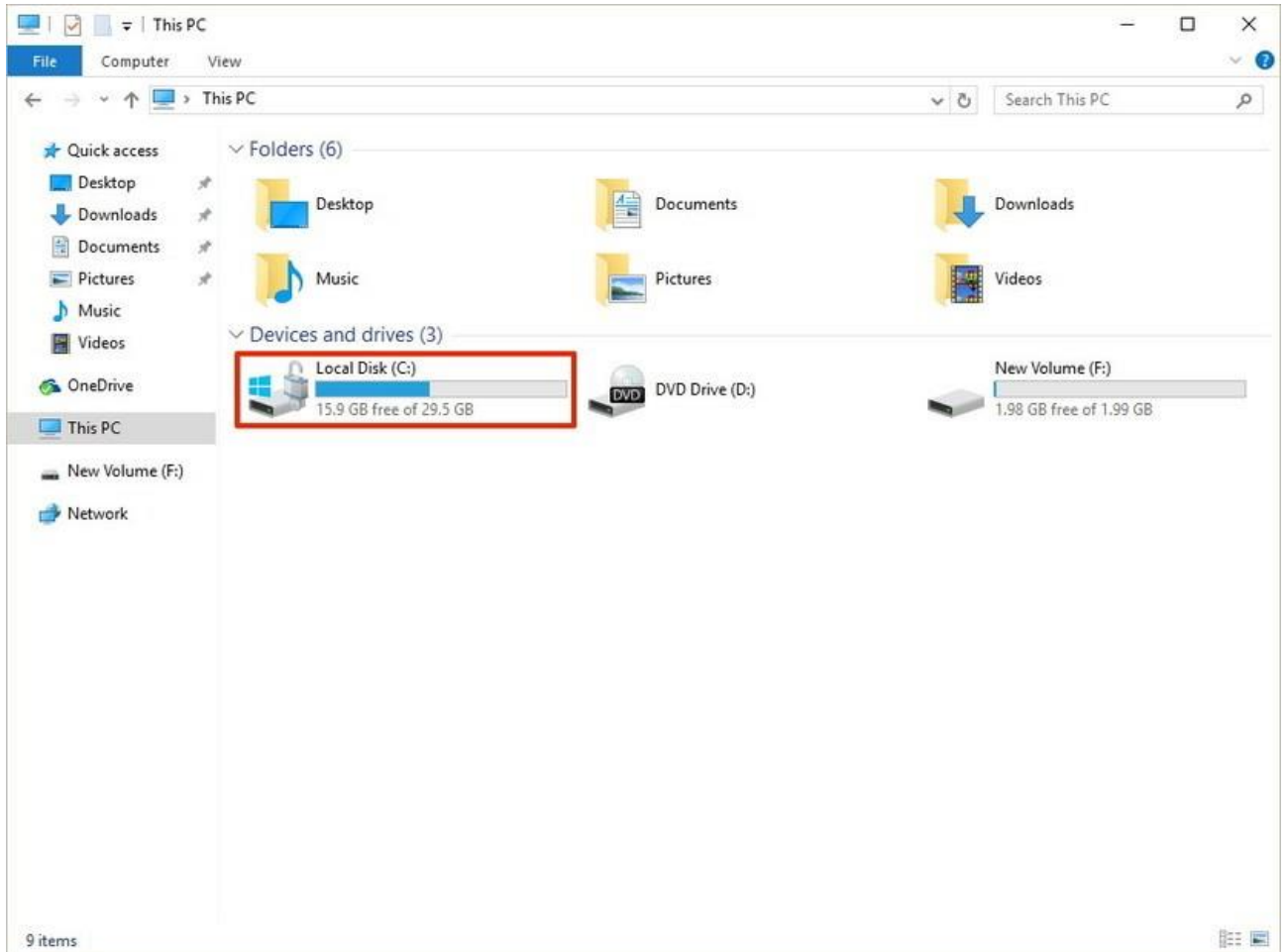
After rebooting, you'll notice that your computer will quickly boot to the Windows 10 desktop. However, if you go to **Control Panel > System and Security > BitLocker Drive Encryption**, you'll see that BitLocker is still encrypting your drive. Depending on the option you selected and the size of the drive, this process can take a long time, but you'll still be able to work on your computer.



Once the encryption process completes, the drive level should read **BitLocker on**.



You can verify that BitLocker is turned on by the lock icon on the drive when you open This PC on File Explorer.

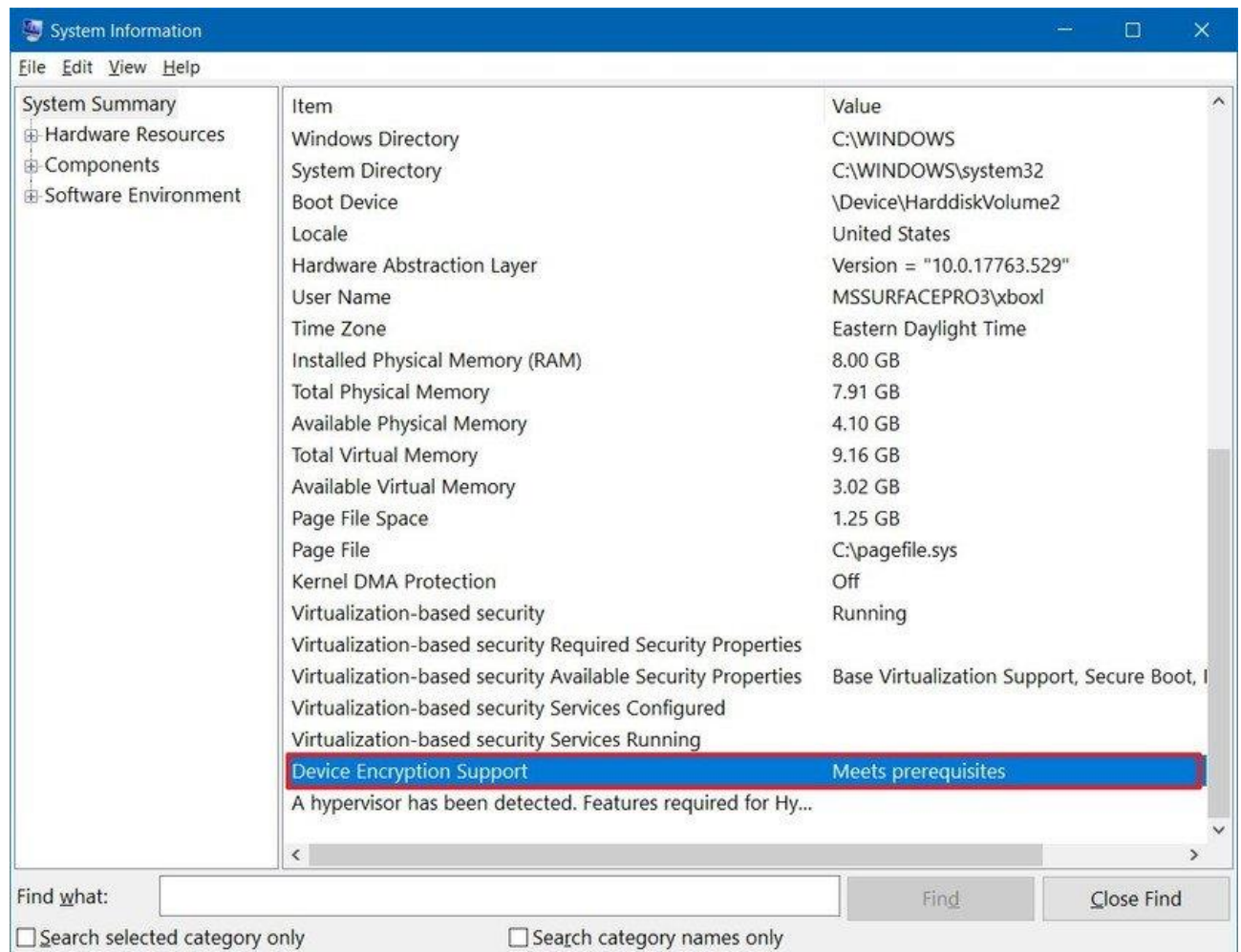


If you use **Windows 10 (Home)** you can use the "device encryption" option, but only if your device meets the hardware requirements:

- Trusted Platform Module (TPM) version 2 with support for Modern Standby;
- TPM must be enabled;
- Unified Extensible Firmware Interface (UEFI) firmware style.

You can check device encryption support:

1. Open **Start**.
2. Search for **System Information**, right-click the top result, and select **the Run as administrator** option.
3. Click the **System Summary** branch from the left pane.
4. Check the "Device Encryption Support" item, and if it reads **Meets prerequisites**, then your computer includes support file encryption.



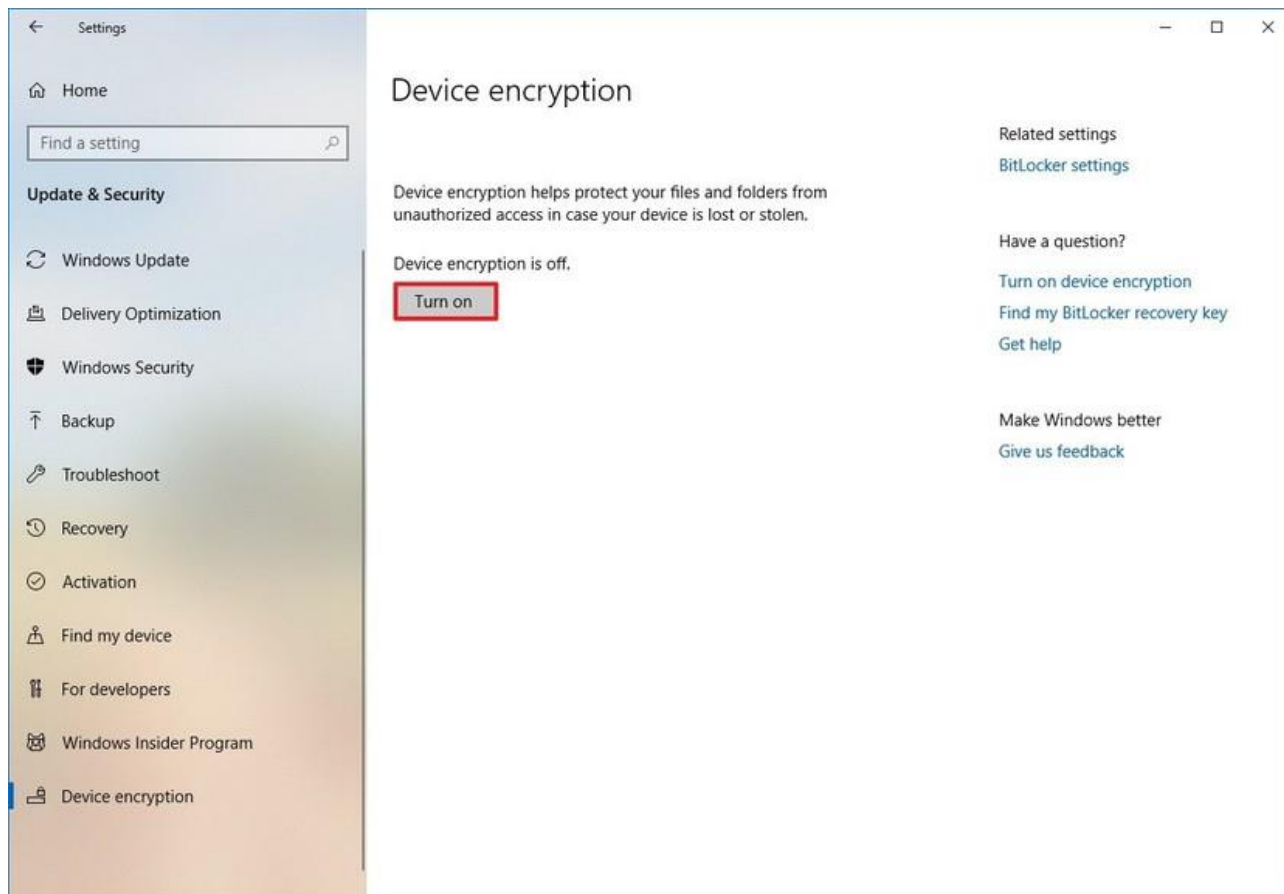
After you complete the steps, you can proceed to enable encryption on the entire system.

For Enable Device Encryption on Windows (**Home**).

1. Open **Settings**.
2. Click on **Update & Security**.
3. Click on **Device encryption**.

**Quick tip:** If the "Device encryption" page isn't available, then it's likely that your device doesn't support the encryption feature.

4. Under the "Device encryption" section, click the **Turn on** button.




Once you complete the steps, Windows 10 will turn on encryption for the current and future files you store on your computer.

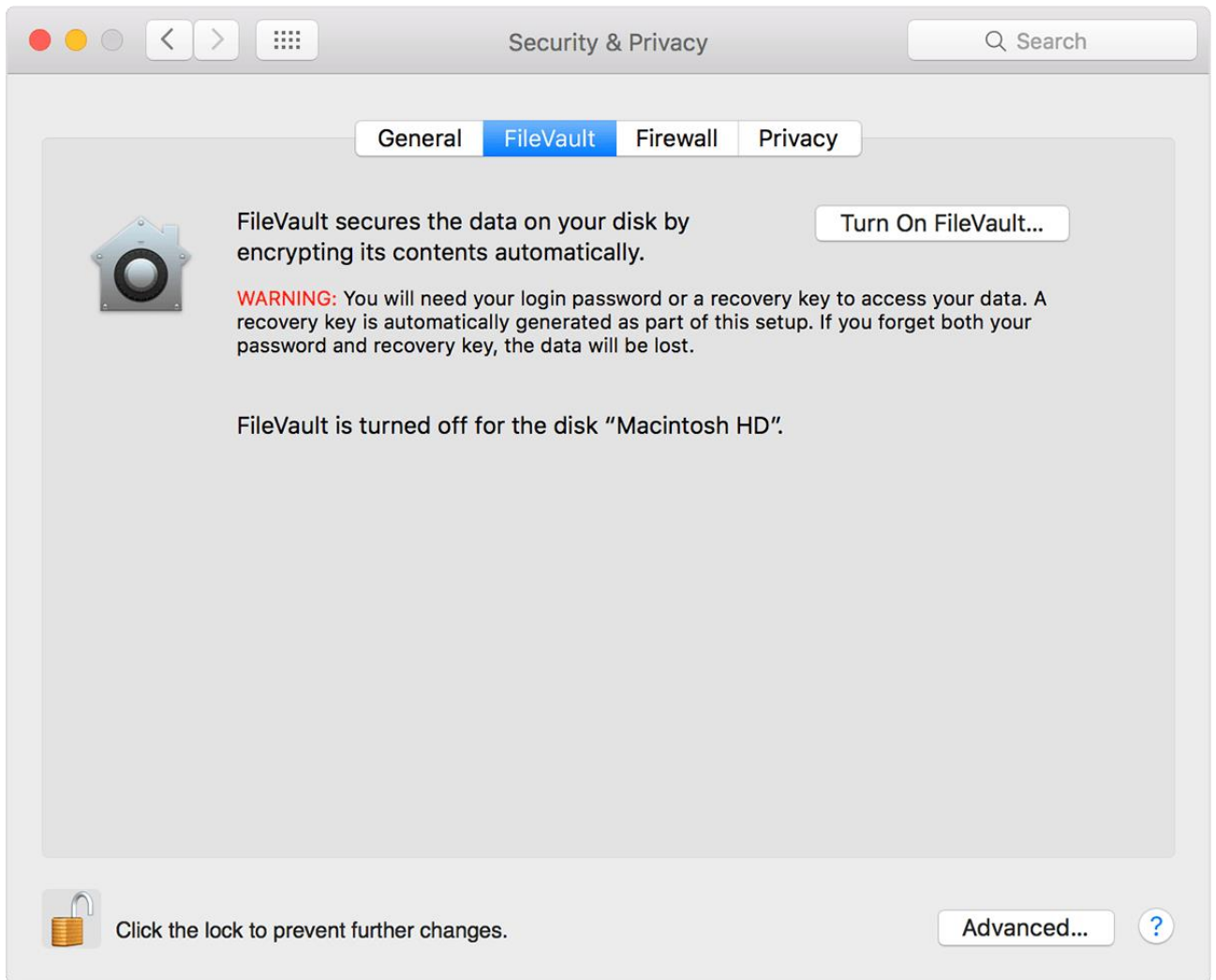
**If the device's encryption option is not available, we recommend you use Dual Boot Setup or request a virtual machine.**

## 2. Encryption Disk for MacOS

For Mac operating systems a FileVault is used that performs disk encryption.

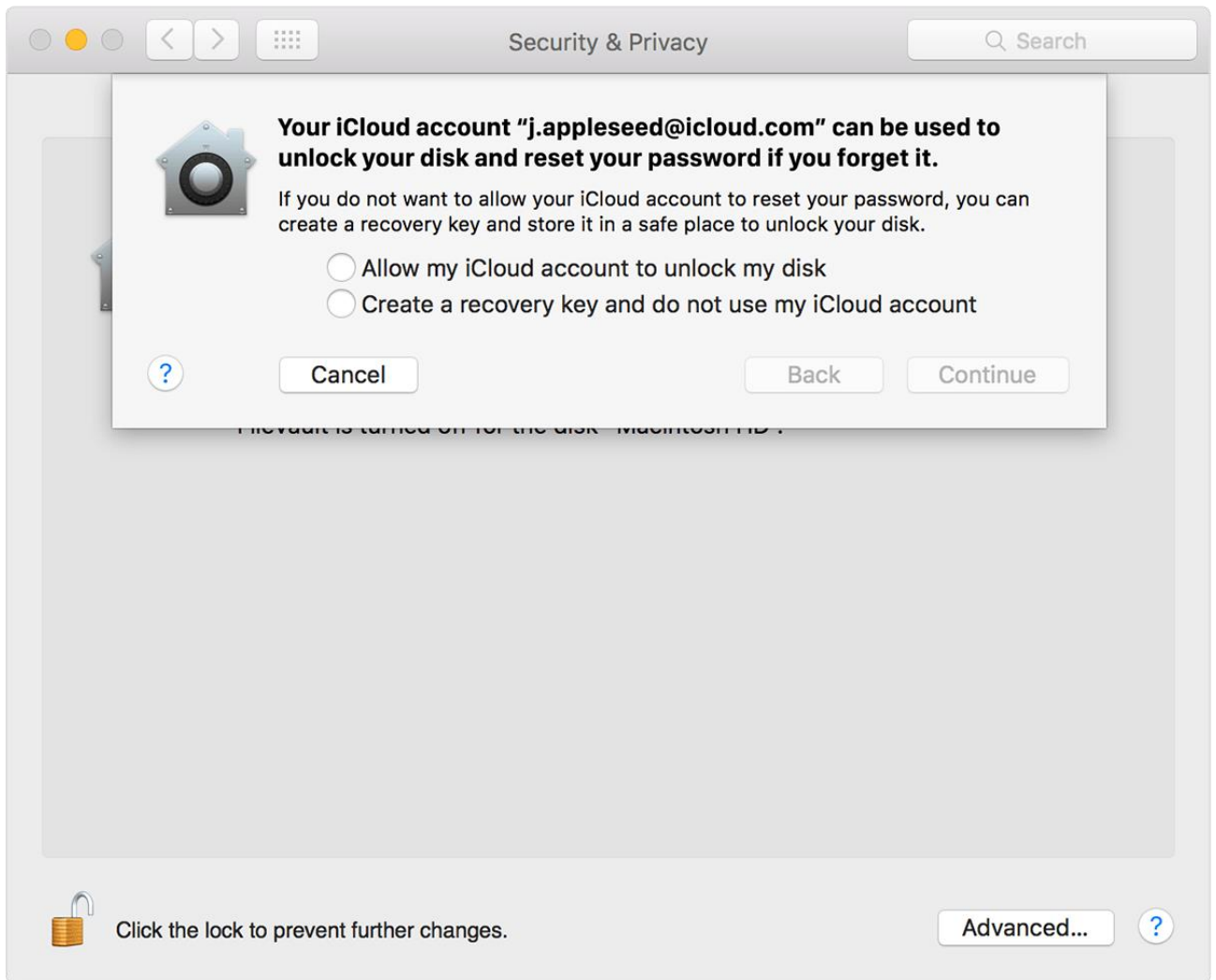
For Enable FileVault on MacOS.

1. Choose Apple menu () > System Preferences, then click Security & Privacy.
2. Click the FileVault tab.
3. Click , then enter an administrator name and password.
4. Click Turn On FileVault.



5. Choose how you want to be able to unlock your disk and reset your password, in case you ever forget your password:






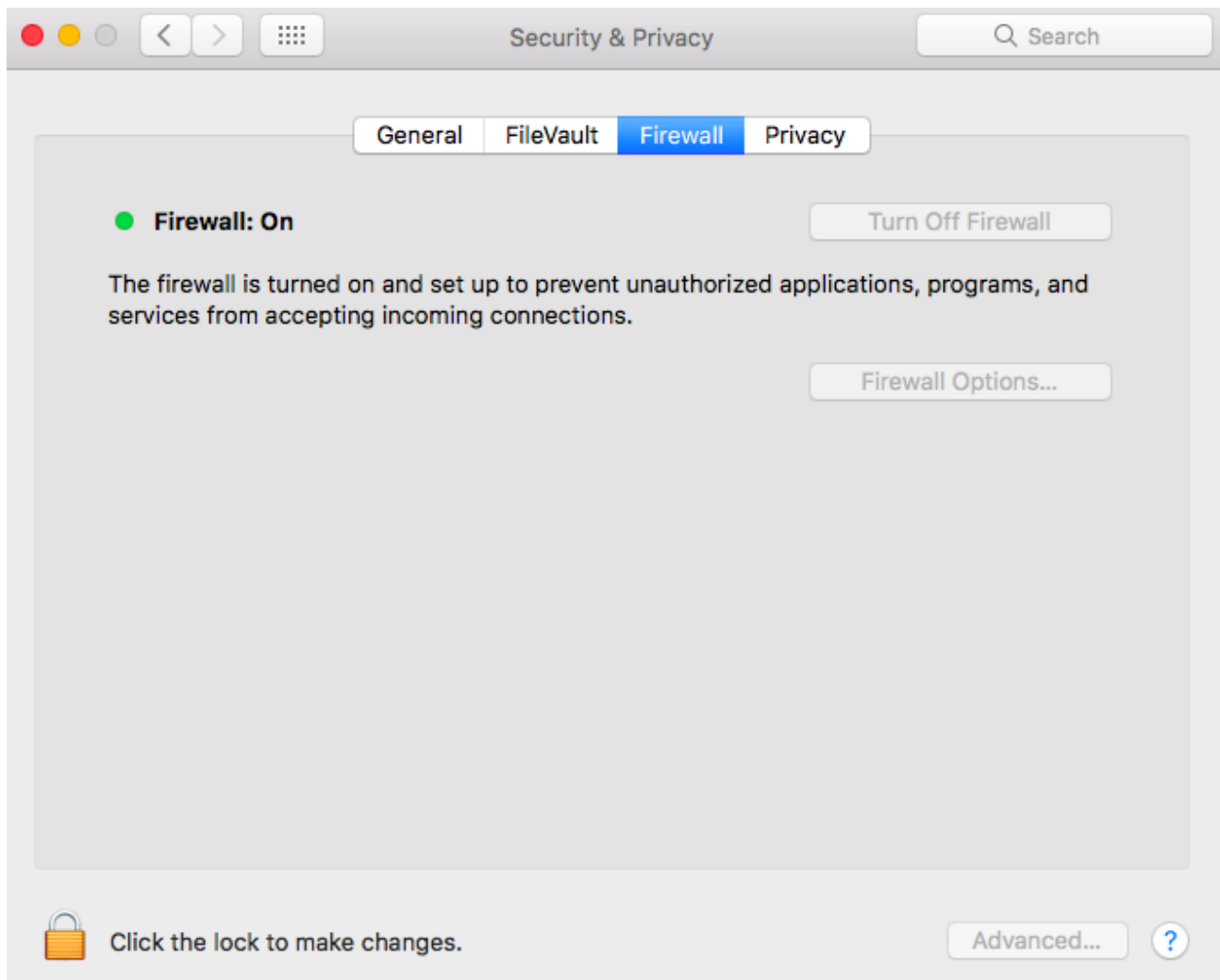
Encryption occurs in the background as you use your Mac, and only while your Mac is awake and plugged in to AC power. You can check progress in the FileVault section of Security & Privacy preferences. Any new files that you create are automatically encrypted as they are saved to your startup disk.

When FileVault setup is complete and you restart your Mac, you will use your account password to unlock your disk and allow your Mac to finish starting up. FileVault requires that you log in every time your Mac starts up, and no account is permitted to log in automatically.

### 3. Firewall for MacOS

For Enable Firewall on MacOS.

1. Choose Apple menu () > System Preferences, then click Security & Privacy.
2. Click the Firewall tab.
3. Click , then enter an administrator name and password.
4. Click Turn On Firewall.



#### 4. Antivirus programs

If you have problems with your antivirus program, for example, it cannot be updated or it is not free, you can download the latest versions from official sites and install them. We suggest you use these antivirus programs:

- AVG AntiVirus FREE;
- Avira Free Antivirus;
- Avast Free Antivirus.

These antivirus programs are free and they are associated with OPSWAT. Also, you can choose your own antivirus program from the list of antimalware that are associated with OPSWAT, by clicking on this link and select a category '**ANTIMALWARE**' - [OPSWAT Antimalware](#)

### STILL NEED HELP?

1. If Windows Defender says that 'The last successful scan was \_ day(s) ago', follow this link and follow these steps - [https://onlinehelp.opswat.com/metaaccess/Windows\\_Defender-no\\_successful\\_scan\\_recently.html](https://onlinehelp.opswat.com/metaaccess/Windows_Defender-no_successful_scan_recently.html)
2. Visit the [OPSWAT FAQ](#) page for more information.
3. If you have any questions or need help, send a request to <https://support.epam.com/esp/ess.do?orderitem=caOpswatAgentMaintenance>