Encryption Process and Procedures

Table of Contents

Introduction

- Why do we need software encryption?
- Online Resources

Pre Encryption Activities

- Process Flow
- Backing up your computer
- Run Chkdsk and Defrag your Hard Drive
- Check version of Windows Operating System

Upgrading to Windows 10 Education

- Use Microsoft Imagine to Upgrade to Windows 10 Education

Enabling Bitlocker Encryption

- What is Bitlocker
- Bitlocker Requirements
- How to turn on Bitlocker
- How to edit settings if you do not have a TPM Chip
- How to deal with concerns

Enabling Filevault for Mac Computers

- Check what O/S do you have
- Enabling Filevault

Introduction

Why do we need software encryption?

The links were created by Arts ISIT, but it should be the same info, in the final copy we can post similar information onto our CS Webpages.

Encryption is vital for ensuring information security, in compliance with the British Columbia Freedom of Information and Protection of Privacy Act (FIPPA) and with UBC's own policies to protect Personally Identifiable Information (see a Quick Overview of UBC Security Policies).

If your computer contains sensitive or personal information, which includes ANY information about students (student numbers, addresses, email addresses, full names, etc.) or UBC employees, you will be in violation of UBC policy if your computer is not encrypted. Any computer that stores UBC email must be encrypted. This applies to all teaching faculty, including sessional lecturers, TAs

Online Resources

- UBC IT Encryption Services
- UBC Policy 104: Acceptable Use and Security of UBC Electronic Information and Systems
- UBC Information Security Manual V2.0

Pre Encryption Activities

Process Flow for Self Encryption

Why Back up your Data?

We highly recommend that you back up your computer on a regular basis. It is highly recommended to back up your data prior to enabling Bitlocker or updating the operating system.

Regularly backing up your computer is a crucial step in ensuring that your information is insured against damage or loss. While anti-virus software can protect you from viruses and other malware, accidents and physical disasters may also affect your files in unforeseen ways. Data may become corrupted or be deleted accidentally. Computers may fail due to hardware issues, system failure, or physical disasters, including theft and power surges.

All devices containing important information should be regularly backed up to UBC network drives and periodically maintained to ensure the backups are successful. If you make frequent and significant changes to your data, you should increase the number of backups.

Back Up Options

While UBC does not offer an official backup service for faculty and staff, there are many straightforward alternatives for preserving your data. Placing your work files on the UBC network via Home Drive ensures that your personal data stays safe, even if something happens to your computer. Workspace is another service offered by UBC IT that allows you to share files with other users. External hard drives are a simple way to store your information in a physical, portable drive, while commercial options offer reliable, intuitive services and automatic backups.

Below are some recommendations for common backup options. Please note that some services violate UBC and provincial policies if used to store Personally Identifiable Information.

Manual Back Up

This can include manually copying your files, and settings from your profile to an external USB Drive, or onto Cloud or other network storage location such as Home Drive or Workspace. You should check beforehand how much data you have before you start backing up to ensure you have enough space. Home Drive and Workspace limits you to 20 GB of free storage.

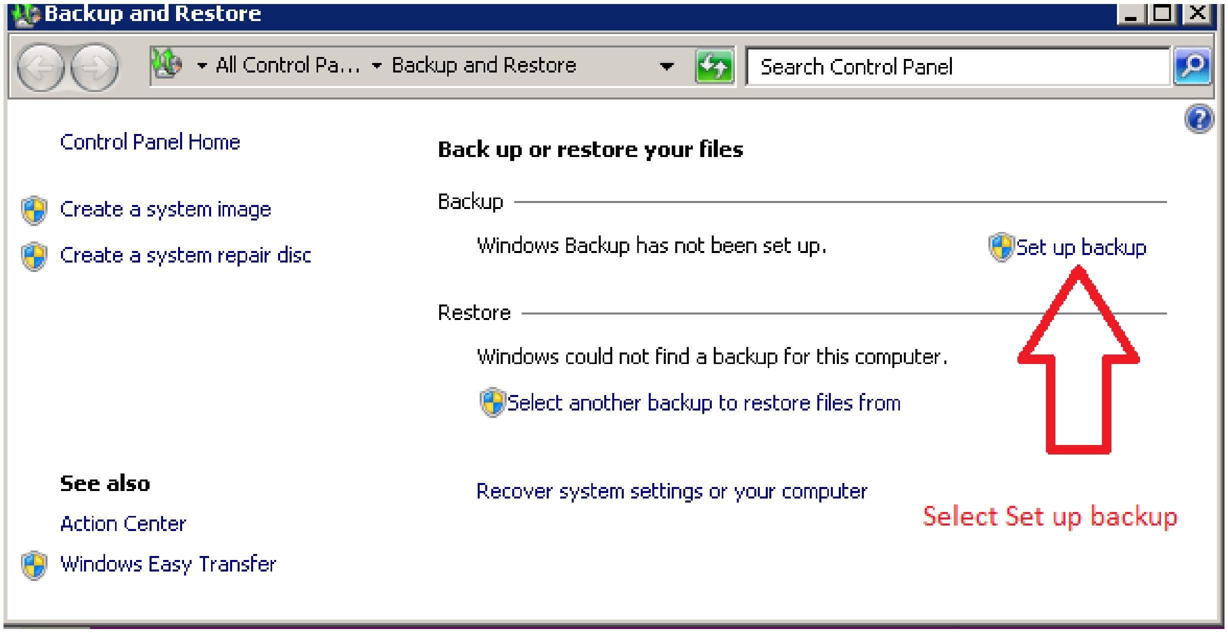
You would copy and paste the files you want to save onto an external source, eg USB Drive, or a Cloud location such as Dropbox.

Windows Back Up

Windows 7 Backup and Restore Application

If you plan on backing up to a USB Drive, insert the drive now

In the search box, type Backup, and the *Backup and Restore* Window will come up.



Back up or restore your files

Backup

Windows Backup has not been set up.

Set up backup

Restore

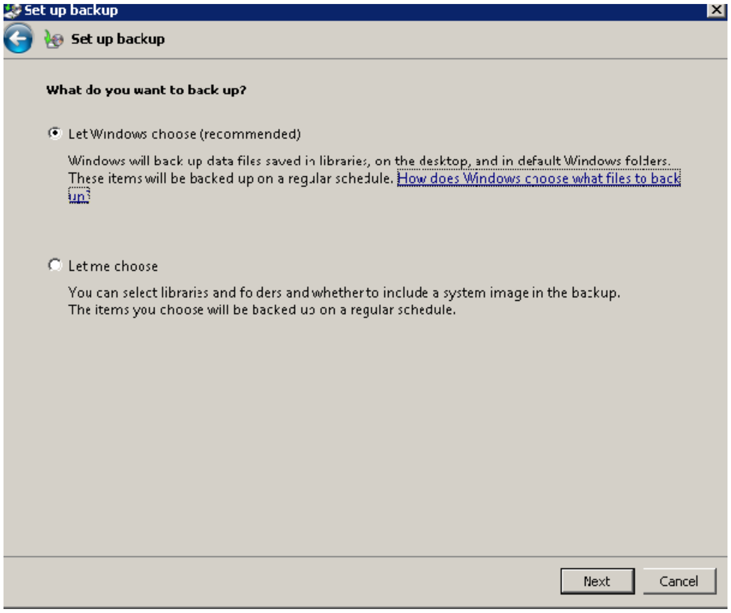
Windows could not find a backup for this computer.

Select another backup to restore files from

Recover system settings or your computer

Select Set up backup

Select the Backup location, such as your USB Drive, or to a network drive, eg, Dropbox
If you are not too sure what to back up, Let Windows choose.



Set up backup

What do you want to back up?

● Let Windows choose (recommended)

Windows will back up data files saved in libraries, on the desktop, and in default Windows folders. These items will be backed up on a regular schedule. How does Windows choose what files to back up?

○ Let me choose

You can select libraries and folders and whether to include a system image in the backup. The items you choose will be backed up on a regular schedule.

Click Next, in the next Windows, Save settings and run back up. The time will depend entirely on how much data needs to be back up.   After backing up you can proceed to the next steps.

Microsoft Bitlocker Encryption

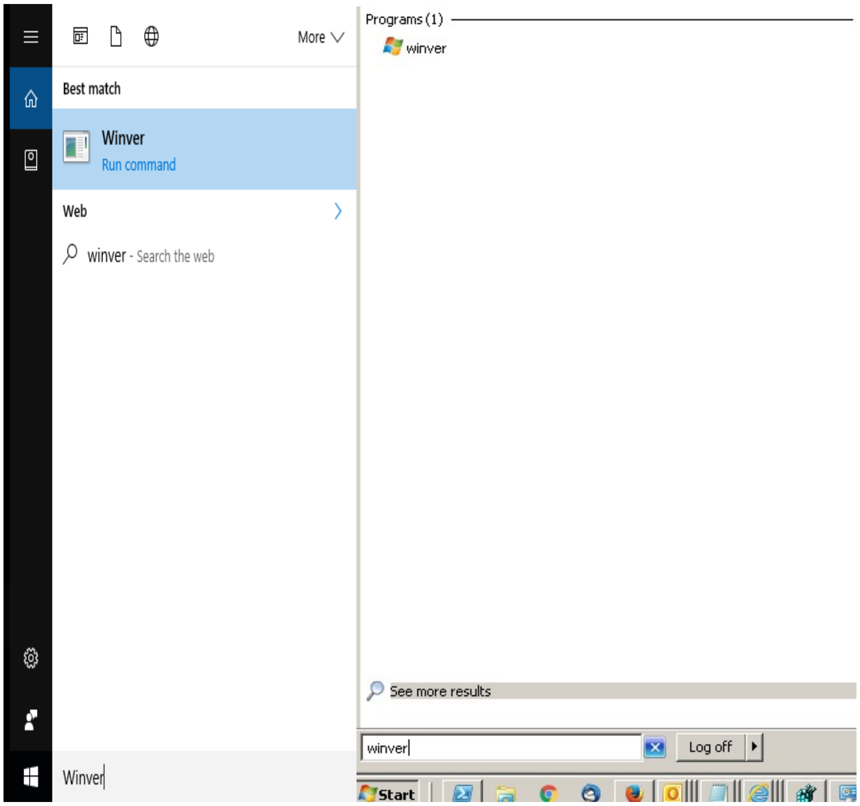
Prior to enabling Bitlocker onto your computer, you need to have the following:

- You must have an administrative credentials on your computer
- You must be able to configure a printer if you want to print the recovery key.
- Your computer must meet BitLocker requirements. This includes:

    - Windows 7, 8, 8.1, Enterprise, Ultimate, Windows 2008 R2, Windows 10 Pro, Enterprise or Education
    - A TPM microchip, version 1.2, turned on for use with BitLocker on operating system drives is recommended for validation of early boot components and storage of the BitLocker master key. If the computer does not have a TPM, a USB flash drive may be used to store the BitLocker key.
    - A Trusted Computing Group (TCG)-compliant BIOS for use with BitLocker on operating system drives.
    - A BIOS setting to start up first from the hard drive, not the USB or CD drives.

What Version of Windows do you have?

Type “**Winver**” without the quotes in the search field. A new Window will appear tell you what version you have. For example.

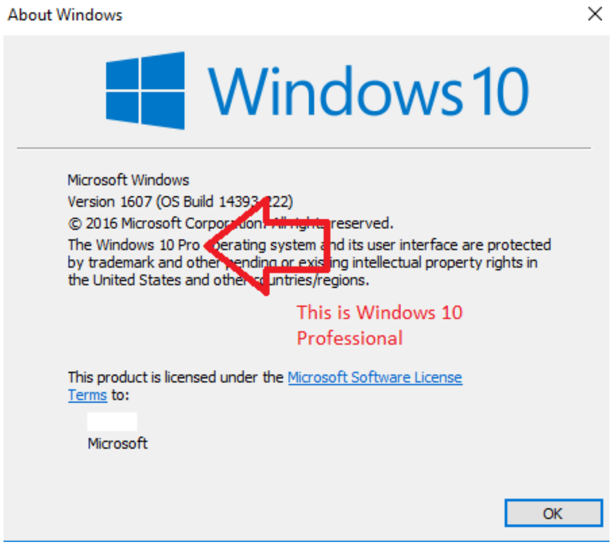


Samples of Windows 10 and Windows 7

After you enter “winver”, and press the return key, a new Window will come up showing you what version you have.

If you have Windows 10 Pro, Enterprise, or Education editions, go to the section on *How to Enable Bitlocker.*

If you have Windows 10 Home Edition, or Windows 7, 8, or 8.1, go to the section on how to Upgrade to Windows 10 Education through Microsoft Imagine

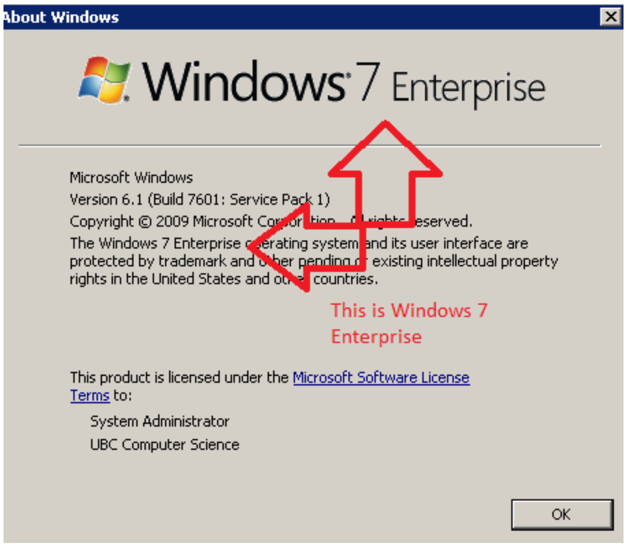


Microsoft Windows
Version 1607 (OS Build 14393.222)
© 2016 Microsoft Corporation. All rights reserved.
The Windows 10 Pro operating system and its user interface are protected by trademark and other pending or existing intellectual property rights in the United States and other countries/regions.

This is Windows 10 Professional

This product is licensed under the Microsoft Software License Terms to:

[redacted]
Microsoft



Microsoft Windows
Version 6.1 (Build 7601: Service Pack 1)
Copyright © 2009 Microsoft Corporation. All rights reserved.
The Windows 7 Enterprise operating system and its user interface are protected by trademark and other pending or existing intellectual property rights in the United States and other countries.

This is Windows 7 Enterprise

This product is licensed under the Microsoft Software License Terms to:

System Administrator
UBC Computer Science

How to Upgrade to Windows 10 Education

To access and upgrade your computer to Windows 10 Education edition, you will need to be a current registered Faulty, Staff, or student. The link to access the software is here:

Imagine Premium link (link is external)

Procedures

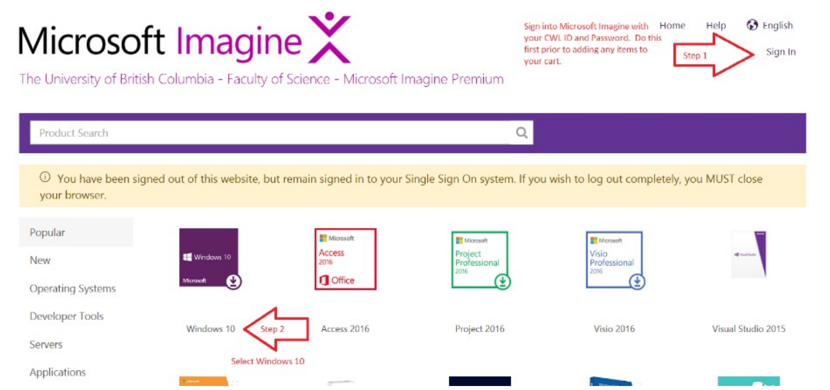
1. Back up your data, see the section on backing up your data.
2. Ensure your hard drive is in good condition by running Disk Clean up, or a disk cleaning utility such as CCleaner. Run Chkdsk /R from a command line. Removing unneeded files and ensuring your hard drive is in good condition will help ensure to upgrade works properly for you.

If there are issues with your hardware, address these first prior to doing any upgrades. If you do not, the upgrade may not work, and you may lose any files that you have.

3. Access the Imagine Premium link here:

   Imagine Premium link (link is external)

4. Click on Sign In, and login with your CWL account and password
5. Select Windows 10



The University of British Columbia - Faculty of Science - Microsoft Imagine Premium

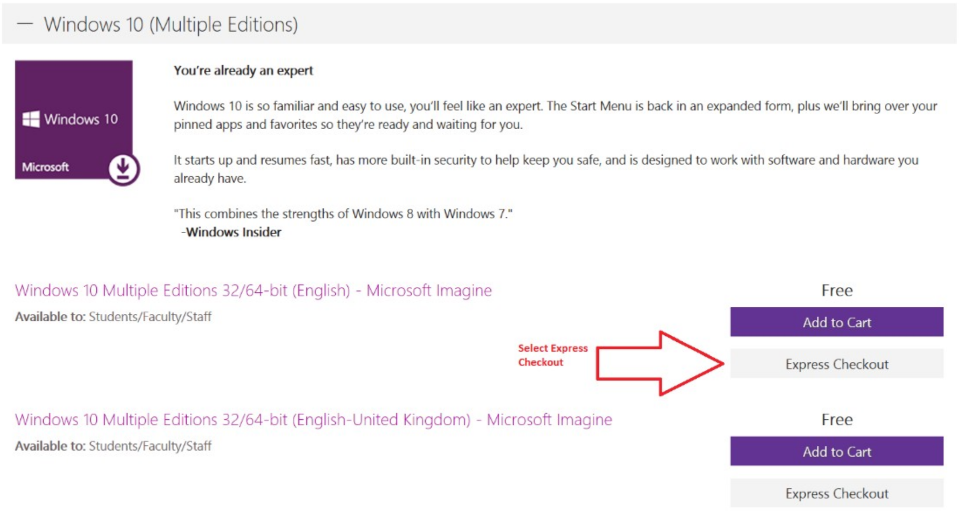
Sign into Microsoft Imagine with your CWL ID and Password. Do this first prior to adding any items to your cart.

Step 1

You have been signed out of this website, but remain signed in to your Single Sign On system. If you wish to log out completely, you MUST close your browser.

Step 2

Select Windows 10



— Windows 10 (Multiple Editions)

You're already an expert

Windows 10 is so familiar and easy to use, you'll feel like an expert. The Start Menu is back in an expanded form, plus we'll bring over your pinned apps and favorites so they're ready and waiting for you.

It starts up and resumes fast, has more built-in security to help keep you safe, and is designed to work with software and hardware you already have.

"This combines the strengths of Windows 8 with Windows 7."
-**Windows Insider**

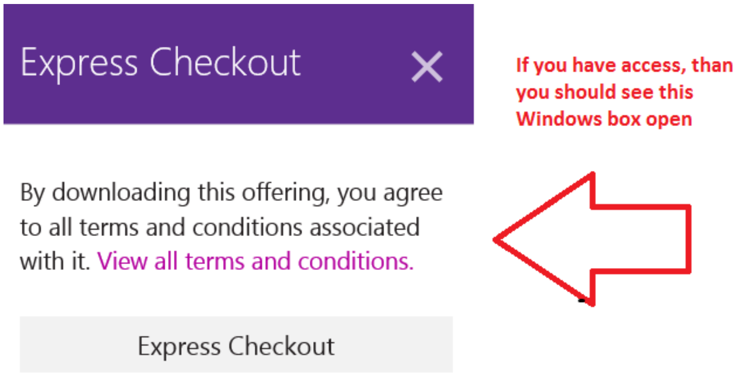
Windows 10 Multiple Editions 32/64-bit (English) - Microsoft Imagine
Available to: Students/Faculty/Staff

Select Express Checkout

Windows 10 Multiple Editions 32/64-bit (English-United Kingdom) - Microsoft Imagine
Available to: Students/Faculty/Staff

6. Select "Windows 10 Multiple Editions 32/64-bit (English) – Microsoft Imagine", and Express Checkout.

7. You should see this Window if you are successful.

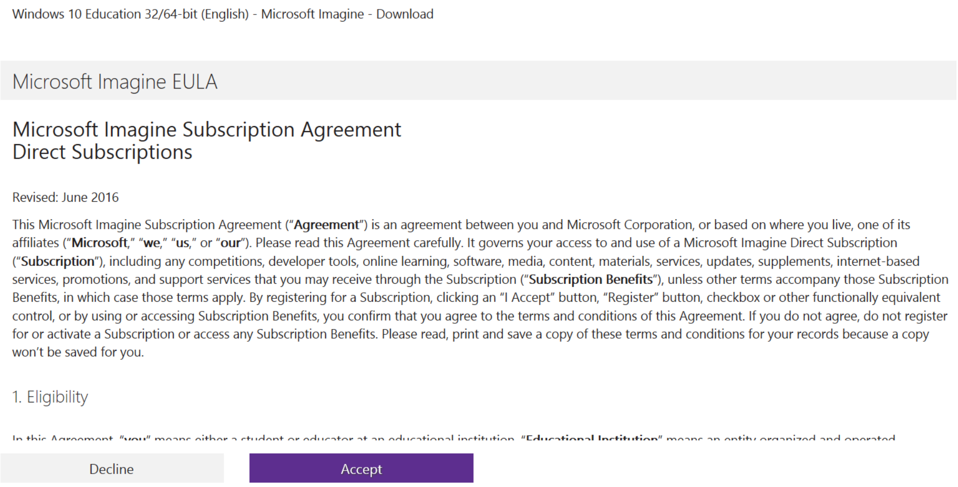


Express Checkout

By downloading this offering, you agree to all terms and conditions associated with it. View all terms and conditions.

If you have access, than you should see this Windows box open

8. Read and accept the Microsoft license agreement.


Windows 10 Education 32/64-bit (English) - Microsoft Imagine - Download

Microsoft Imagine EULA

Microsoft Imagine Subscription Agreement
Direct Subscriptions

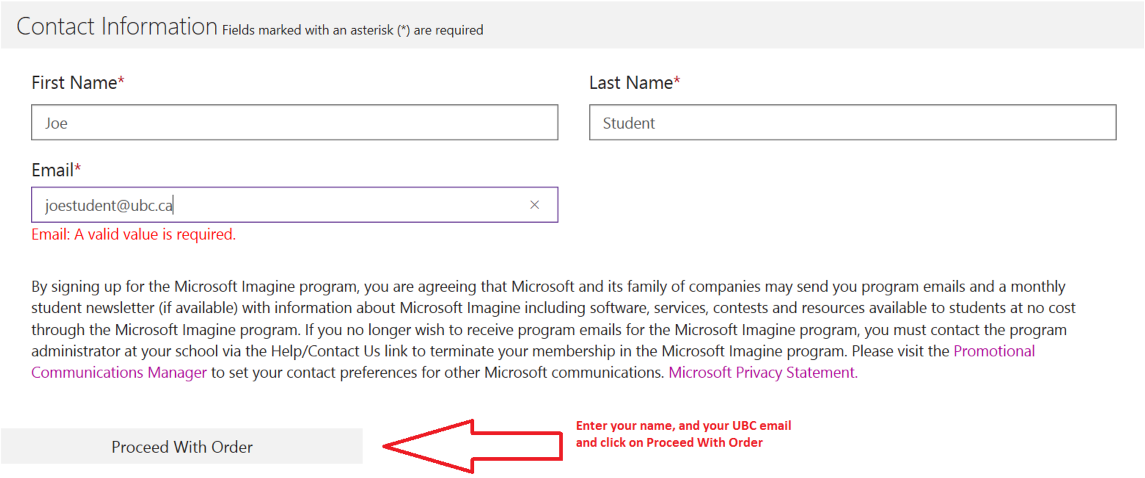
Revised: June 2016

This Microsoft Imagine Subscription Agreement ("**Agreement**") is an agreement between you and Microsoft Corporation, or based on where you live, one of its affiliates ("**Microsoft**," "**we**," "**us**," or "**our**"). Please read this Agreement carefully. It governs your access to and use of a Microsoft Imagine Direct Subscription ("**Subscription**"), including any competitions, developer tools, online learning, software, media, content, materials, services, updates, supplements, internet-based services, promotions, and support services that you may receive through the Subscription ("**Subscription Benefits**"), unless other terms accompany those Subscription Benefits, in which case those terms apply. By registering for a Subscription, clicking an "I Accept" button, "Register" button, checkbox or other functionally equivalent control, or by using or accessing Subscription Benefits, you confirm that you agree to the terms and conditions of this Agreement. If you do not agree, do not register for or activate a Subscription or access any Subscription Benefits. Please read, print and save a copy of these terms and conditions for your records because a copy won't be saved for you.

1. Eligibility

In this Agreement, "**you**" means either a student or educator at an educational institution. "**Educational Institution**" means an entity organized and operated

9. Enter your name, work email and click on "Proceed With Order"


Contact Information Fields marked with an asterisk (*) are required

First Name* Joe

Last Name* Student

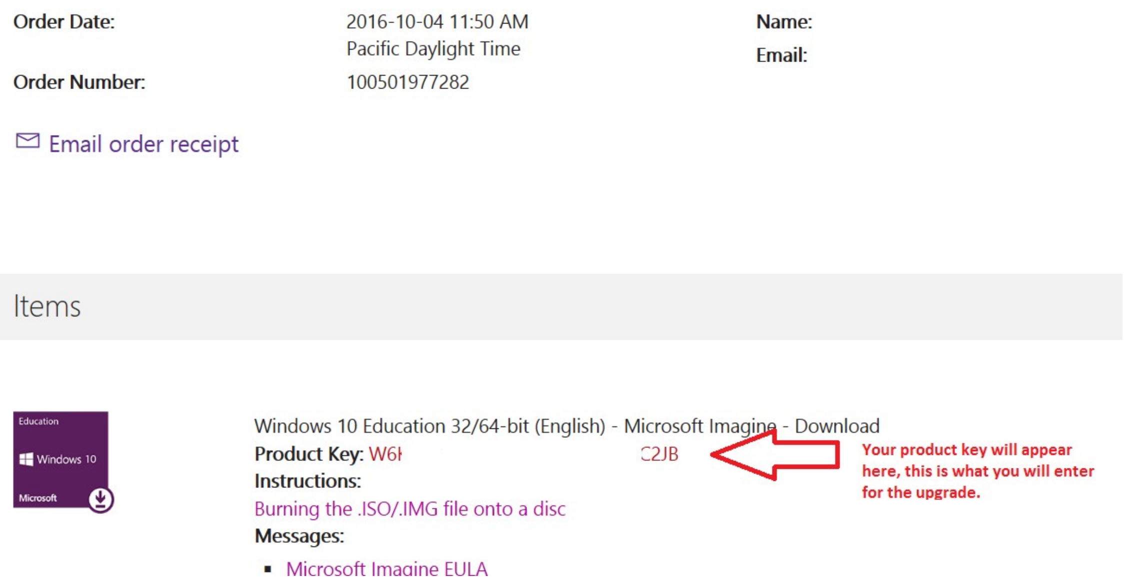
Email* joestudent@ubc.ca

Email: A valid value is required.

By signing up for the Microsoft Imagine program, you are agreeing that Microsoft and its family of companies may send you program emails and a monthly student newsletter (if available) with information about Microsoft Imagine including software, services, contests and resources available to students at no cost through the Microsoft Imagine program. If you no longer wish to receive program emails for the Microsoft Imagine program, you must contact the program administrator at your school via the Help/Contact Us link to terminate your membership in the Microsoft Imagine program. Please visit the Promotional Communications Manager to set your contact preferences for other Microsoft communications. Microsoft Privacy Statement.

Enter your name, and your UBC email and click on Proceed With Order

10. A new windows will open with the license key and download information. You will need the key for the upgrade. Print, take a photo, and/or write down this key.



Order Date: 2016-10-04 11:50 AM Pacific Daylight Time

Order Number: 100501977282

Name:

Email:

Email order receipt

Items

Windows 10 Education 32/64-bit (English) - Microsoft Imagine - Download

Product Key: W6I[redacted]C2JB

Instructions:

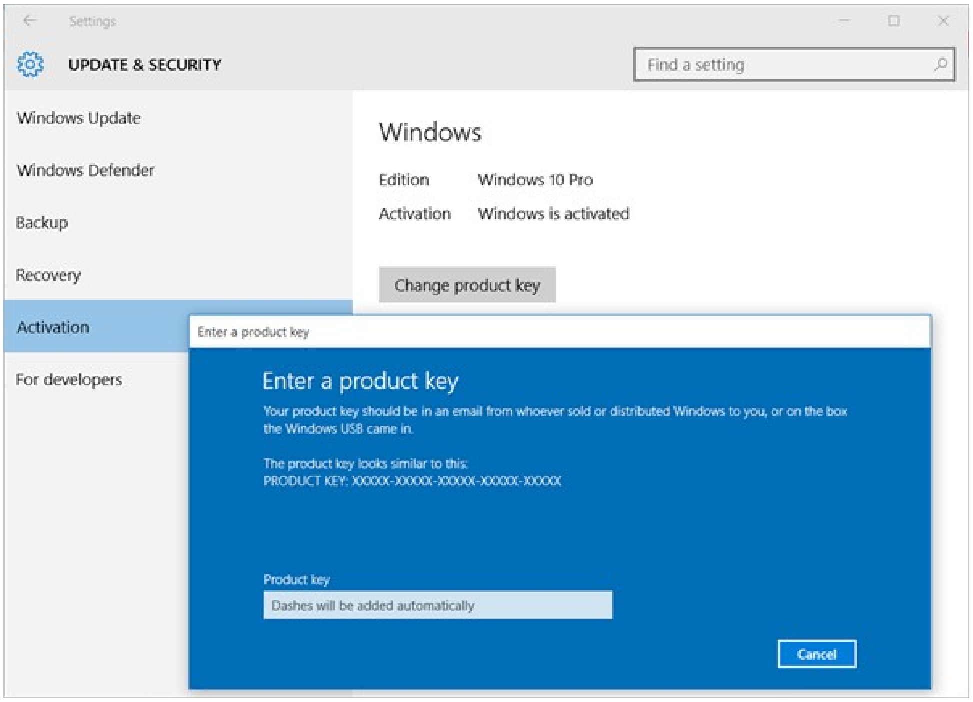
Burning the .ISO/.IMG file onto a disc

Messages:

- Microsoft Imagine EULA

Your product key will appear here, this is what you will enter for the upgrade.

Once you have the key, you can do the upgrade. **Basic Windows Key Change Process:**
Open Start > Settings app > Update and Security. Select Activation, in the left panel. Here you will see the activation status. If all has gone smoothly, Windows 10 should have taken your Windows 7 or Windows 8.1 product key and activated itself automatically.



Windows

Edition Windows 10 Pro

Activation Windows is activated

Enter a product key

Enter a product key

Your product key should be in an email from whoever sold or distributed Windows to you, or on the box the Windows USB came in.

The product key looks similar to this:
PRODUCT KEY: XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

Product key

Dashes will be added automatically

11. **Important – during the install process, it will ask, do you want to "keep personal files and apps", select Yes, otherwise ALL your data and apps will be erased.**
12. If it is successful, the install will complete, and will ask you to restart the computer one or more times. Check your files and settings and they should all be there.
13. Now you can proceed with enabling Bitlocker onto your computer.

What if entering the upgrade key does not work?

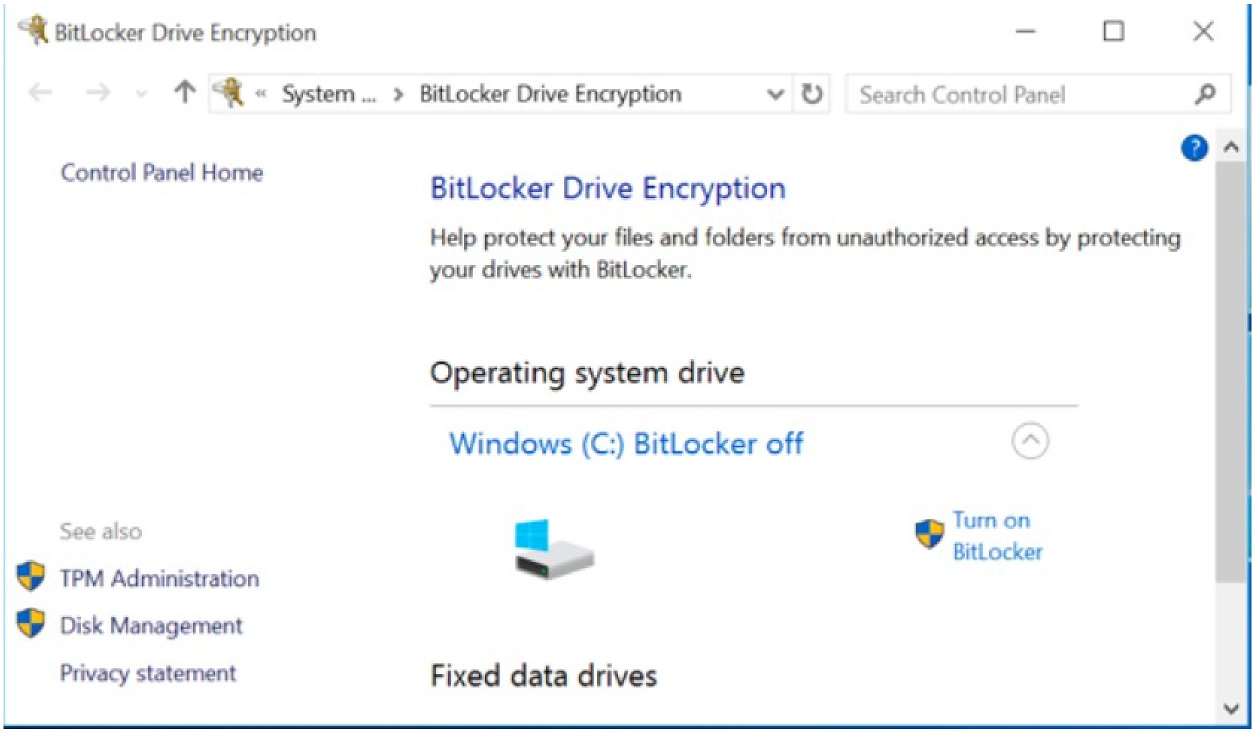
There are different scenarios where the install may not work.

Installation is stuck at eg, 0% and does not proceed over a long time. Ctrl-Alt-Del to stop the process and restart your computer. Stop any other applications that are running, eg, Skype, etc, re-run your disk clean up and chkdsk /r and try again.

If it fails again, you can burn the Windows 10 iso onto a DVD, you will need a DVD-RW Drive to do this and a blank DVD. Try the install from the DVD.

If this still does not work, do not proceed with the upgrade.

Enabling Bitlocker – Windows 7 Enterprise, Ultimate, Windows 10 Pro, Enterprise or Education Editions



BitLocker Drive Encryption

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

To turn on BitLocker Drive Encryption on a fixed or removable data drive

1. Click **Start**, click **Control Panel**, click **System and Security**, and then click **BitLocker Drive Encryption**.
2. Click **Turn On BitLocker** for the fixed or removable data drive that you want to encrypt.

The BitLocker setup wizard will ask you how you want to unlock the drive. Fixed data drives can be configured to automatically unlock with the operating system drive is encrypted, to unlock after a password is supplied, or to unlock after a smart card is inserted.

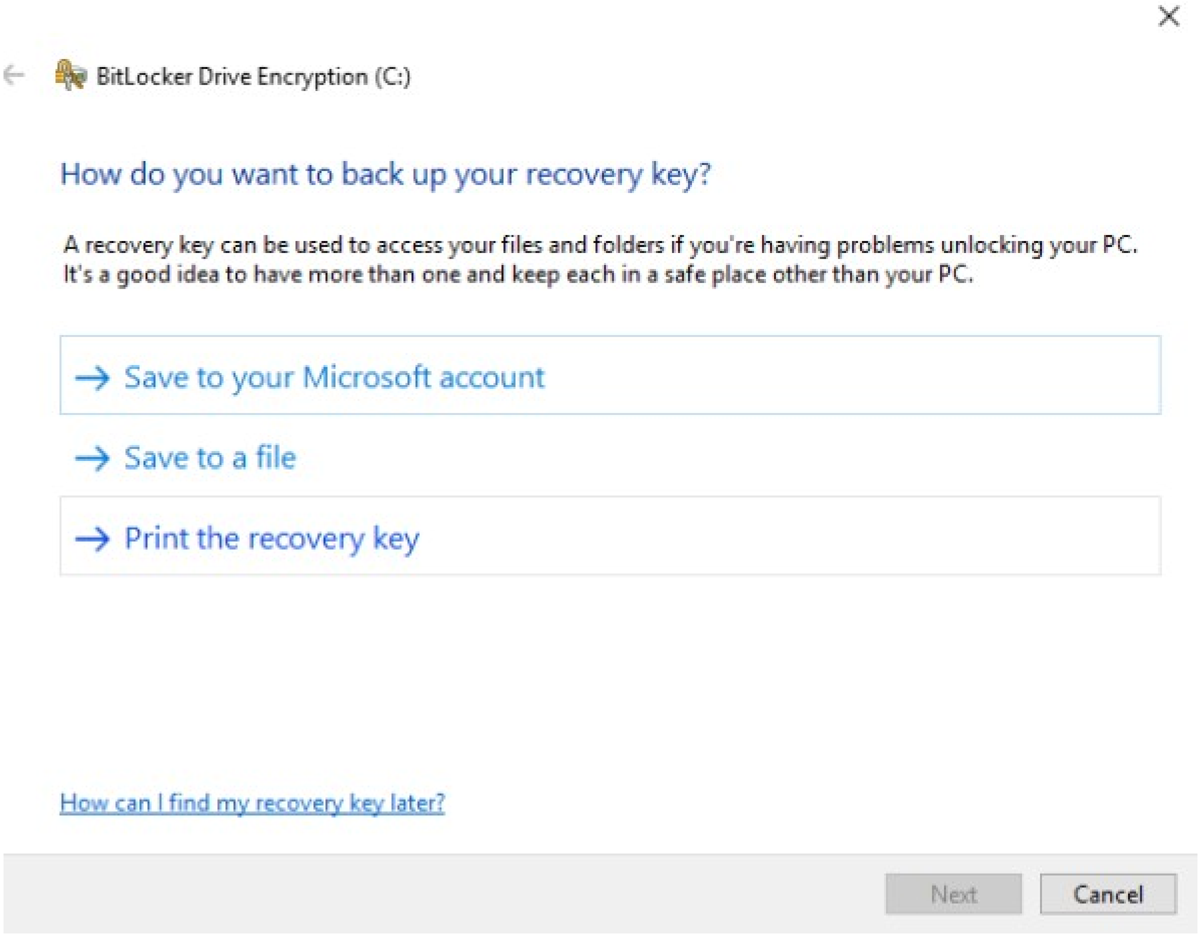
Removable data drives can be configured to unlock after a password is supplied or to unlock after a smart card is inserted. If you want the removable data drive to automatically unlock you can specify the option after encryption has occurred by clicking **Manage BitLocker** from the **BitLocker Drive Encryption** Control Panel or by selecting the A**utomatically unlock on this computer from now on** check box when you unlock the drive.

Before BitLocker encrypts the drive, the BitLocker setup wizard prompts you to choose how to store the recovery key. You can choose from the following options:

- **Save the recovery key to a USB flash drive**. Saves the recovery key to a USB flash drive. This option cannot be used with removable drives.

- **Save the recovery key to a file**. Saves the recovery key to a network drive or other location.

- **Print the recovery key**. Prints the recovery key.



BitLocker Drive Encryption (C:)

How do you want to back up your recovery key?

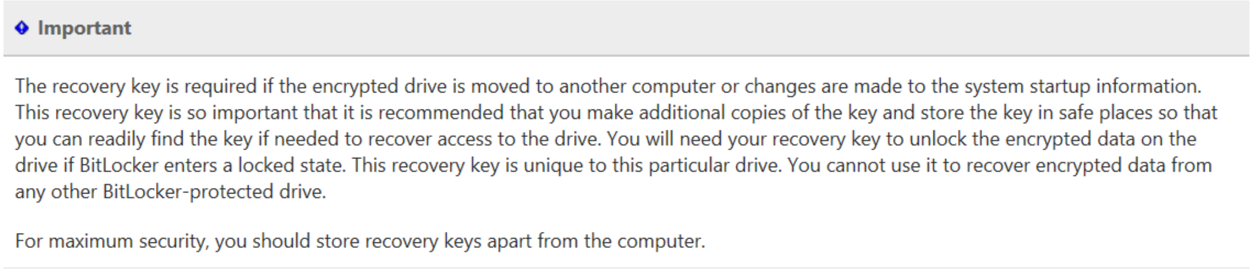
A recovery key can be used to access your files and folders if you're having problems unlocking your PC. It's a good idea to have more than one and keep each in a safe place other than your PC.

Save to your Microsoft account
Save to a file
Print the recovery key
How can I find my recovery key later?
Next
Cancel

Use one or more of these options to preserve the recovery key. For each option that you select, follow the wizard steps to set the location for saving or printing the recovery key. When you have finished saving the recovery key, click **Next**.

1. The BitLocker setup wizard asks if you are ready to encrypt the drive. Click Start Encrypting.
2. The Encrypting status bar is displayed. You can monitor the ongoing completion status of the drive encryption by moving the mouse pointer over the BitLocker Drive Encryption icon in the notification area, at the far right of the taskbar.

By completing this procedure, you have encrypted a fixed or removable data drive, associated a key protector with an unlock method for the drive, and created a recovery key that is unique to this drive.



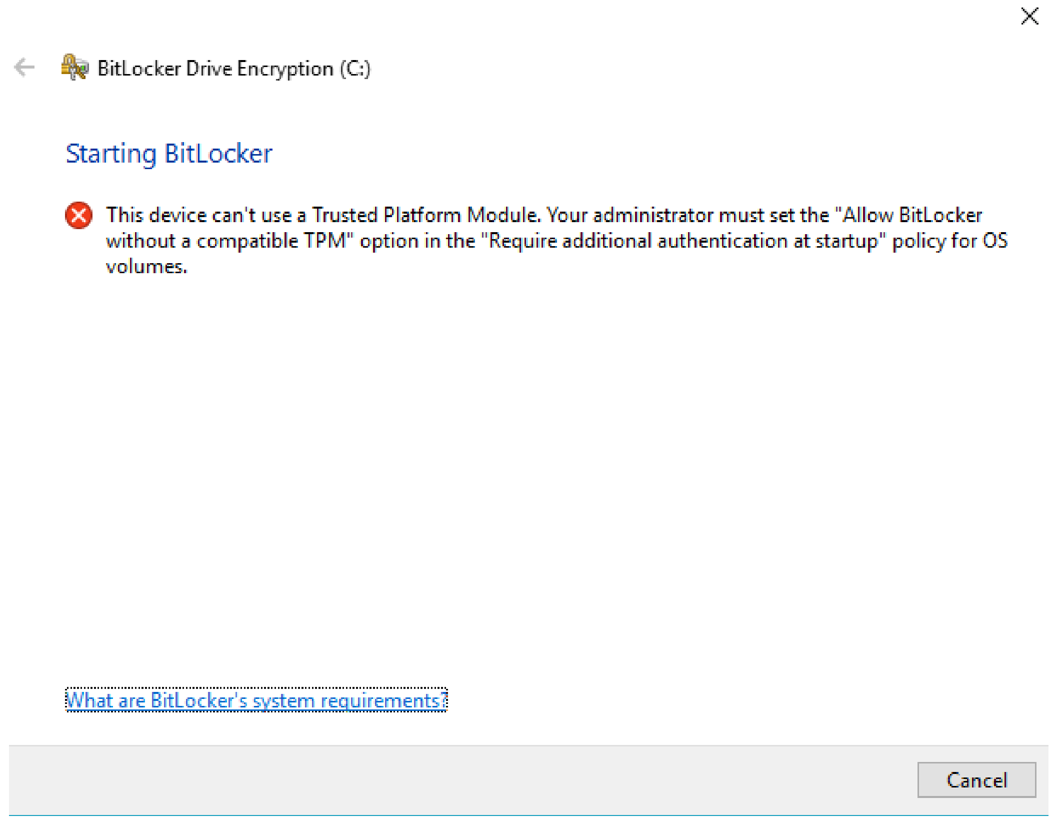
Important

The recovery key is required if the encrypted drive is moved to another computer or changes are made to the system startup information. This recovery key is so important that it is recommended that you make additional copies of the key and store the key in safe places so that you can readily find the key if needed to recover access to the drive. You will need your recovery key to unlock the encrypted data on the drive if BitLocker enters a locked state. This recovery key is unique to this particular drive. You cannot use it to recover encrypted data from any other BitLocker-protected drive.

For maximum security, you should store recovery keys apart from the computer.

No TPM Chip?

If you receive the following message, “This device can’t use a Trusted Platform Module. Your administrator must set the ‘Allow BitLocker without a compatible TPM’ option in the “Require additional authentication at startup ‘policy for OS volumes’, your computer does not have a TPM chip inside.



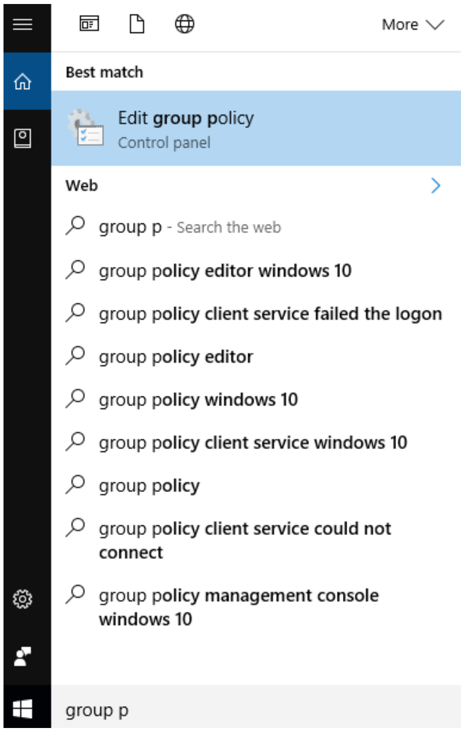
BitLocker Drive Encryption (C:)

Starting BitLocker

This device can't use a Trusted Platform Module. Your administrator must set the "Allow BitLocker without a compatible TPM" option in the "Require additional authentication at startup" policy for OS volumes.

You will need to use the Local Group Policy Editor for setting the policy which allows you to use Bitlocker encryption without a TPM Chip.

Click on the search box, and type “Group policy” and select “**Edit group policy**”.



More

Best match

Edit group policy
Control panel

Web

group p - Search the web

group policy editor windows 10

group policy client service failed the logon

group policy editor

group policy windows 10

group policy client service windows 10

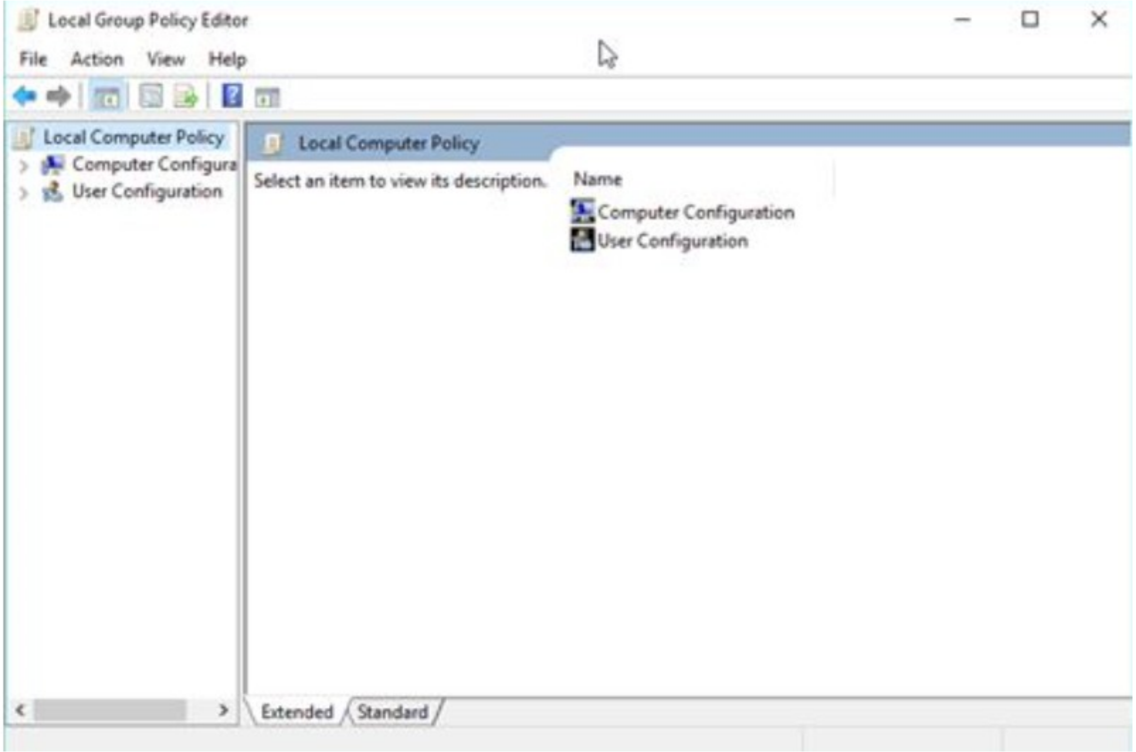
group policy

group policy client service could not connect

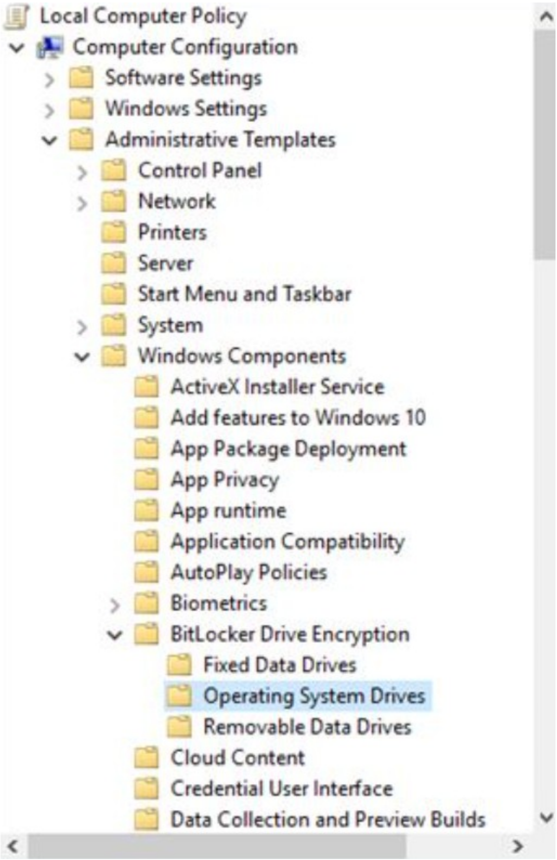
group policy management console windows 10

group p

How to modify the BitLocker Drive Encryption policy

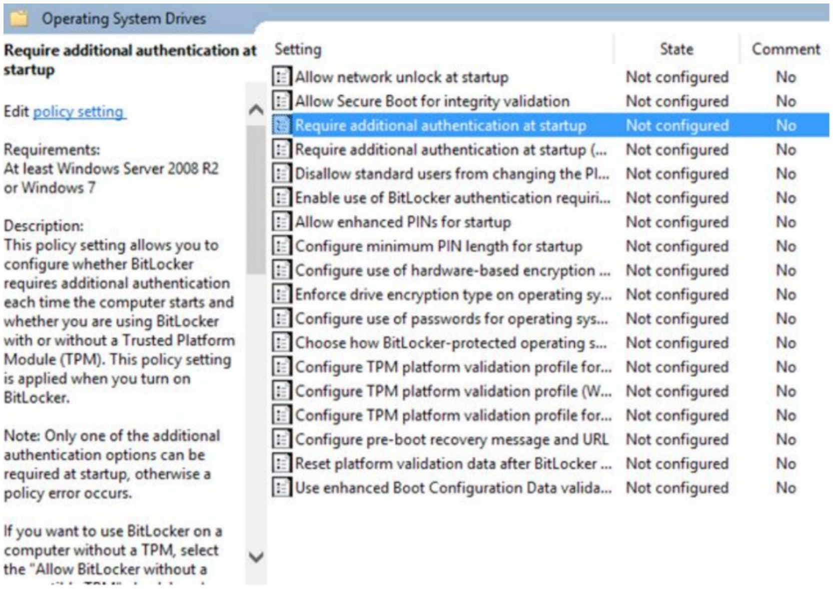


On the left-hand panel, go to the Computer Configuration section and open the following folders: **“Administrative Templates> Windows Components > BitLocker Drive Encryption > Operating System Drives”.**



- Local Computer Policy
  - Computer Configuration
    - Software Settings
    - Windows Settings
    - Administrative Templates
      - Control Panel
      - Network
      - Printers
      - Server
      - Start Menu and Taskbar
      - System
      - Windows Components
        - ActiveX Installer Service
        - Add features to Windows 10
        - App Package Deployment
        - App Privacy
        - App runtime
        - Application Compatibility
        - AutoPlay Policies
        - Biometrics
        - BitLocker Drive Encryption
          - Fixed Data Drives
          - Operating System Drives
          - Removable Data Drives
        - Cloud Content
        - Credential User Interface
        - Data Collection and Preview Builds

Look at the right hand panel and for a setting named: "Require additional authentication at startup". Click on it to open this setting.



Operating System Drives

Require additional authentication at startup

Edit policy setting

Requirements:
At least Windows Server 2008 R2 or Windows 7

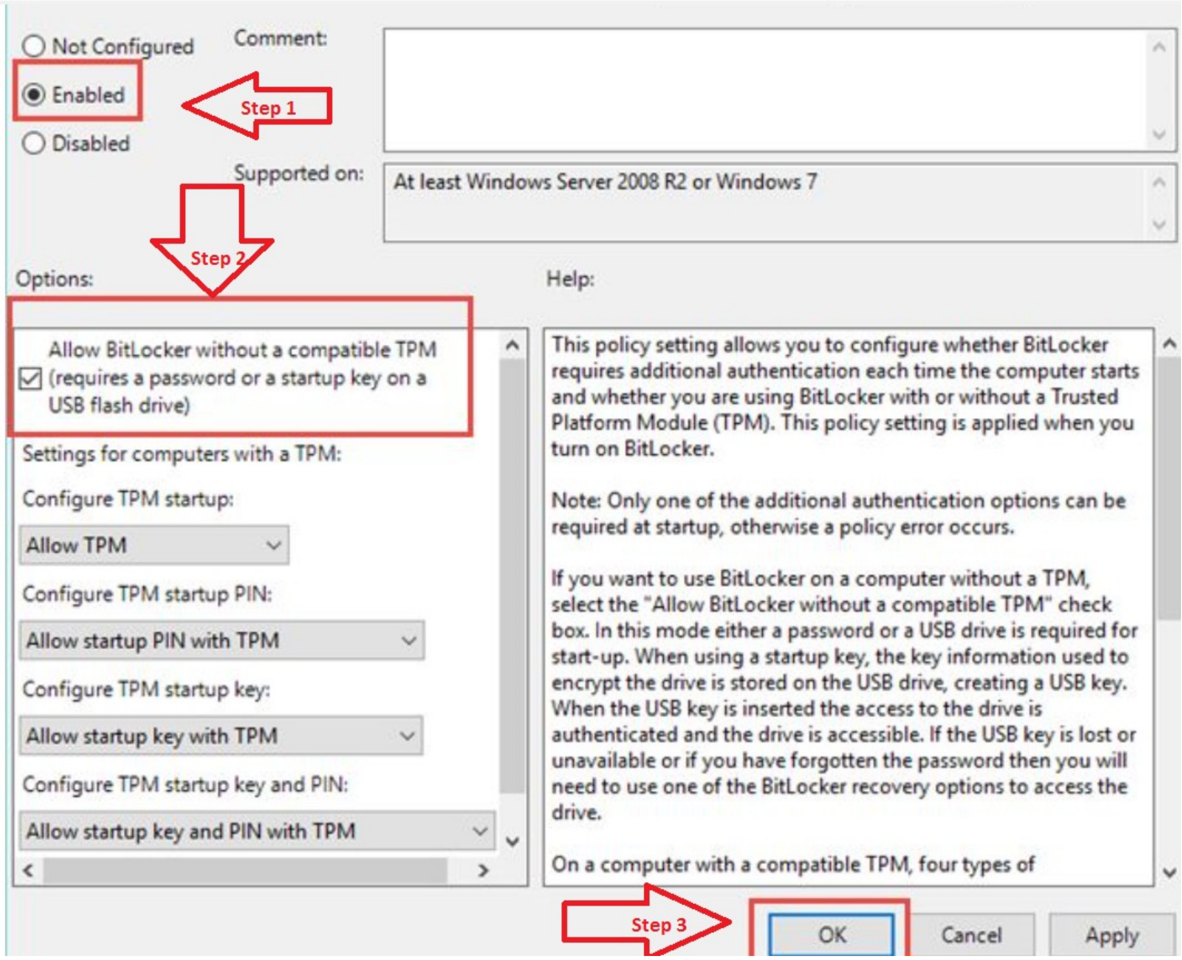
Description:
This policy setting allows you to configure whether BitLocker requires additional authentication each time the computer starts and whether you are using BitLocker with or without a Trusted Platform Module (TPM). This policy setting is applied when you turn on BitLocker.

Note: Only one of the additional authentication options can be required at startup, otherwise a policy error occurs.

If you want to use BitLocker on a computer without a TPM, select the "Allow BitLocker without a

Setting	State	Comment
Allow network unlock at startup	Not configured	No
Allow Secure Boot for integrity validation	Not configured	No
Require additional authentication at startup	Not configured	No
Require additional authentication at startup (...	Not configured	No
Disallow standard users from changing the PI...	Not configured	No
Enable use of BitLocker authentication requiri...	Not configured	No
Allow enhanced PINs for startup	Not configured	No
Configure minimum PIN length for startup	Not configured	No
Configure use of hardware-based encryption ...	Not configured	No
Enforce drive encryption type on operating sy...	Not configured	No
Configure use of passwords for operating sys...	Not configured	No
Choose how BitLocker-protected operating s...	Not configured	No
Configure TPM platform validation profile for...	Not configured	No
Configure TPM platform validation profile (W...	Not configured	No
Configure TPM platform validation profile for...	Not configured	No
Configure pre-boot recovery message and URL	Not configured	No
Reset platform validation data after BitLocker ...	Not configured	No
Use enhanced Boot Configuration Data valida...	Not configured	No

A Window with the properties of this policy is shown. Change the value of this policy to ***Enabled.*** Then, check the option which says "Allow BitLocker without a compatible TPM" and press OK.



○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Server 2008 R2 or Windows 7

Options:

☑ Allow BitLocker without a compatible TPM (requires a password or a startup key on a USB flash drive)

Settings for computers with a TPM:

Configure TPM startup: Allow TPM

Configure TPM startup PIN: Allow startup PIN with TPM

Configure TPM startup key: Allow startup key with TPM

Configure TPM startup key and PIN: Allow startup key and PIN with TPM

Help:

This policy setting allows you to configure whether BitLocker requires additional authentication each time the computer starts and whether you are using BitLocker with or without a Trusted Platform Module (TPM). This policy setting is applied when you turn on BitLocker.

Note: Only one of the additional authentication options can be required at startup, otherwise a policy error occurs.

If you want to use BitLocker on a computer without a TPM, select the "Allow BitLocker without a compatible TPM" check box. In this mode either a password or a USB drive is required for start-up. When using a startup key, the key information used to encrypt the drive is stored on the USB drive, creating a USB key. When the USB key is inserted the access to the drive is authenticated and the drive is accessible. If the USB key is lost or unavailable or if you have forgotten the password then you will need to use one of the BitLocker recovery options to access the drive.

On a computer with a compatible TPM, four types of

When done, close the Local Group Policy Editor window. You can now use BitLocker to encrypt your system drive without having a TPM chip in your computer.

How to Deal with Concerns?

What support service will be in place for TAs if they have technical issues or concerns?

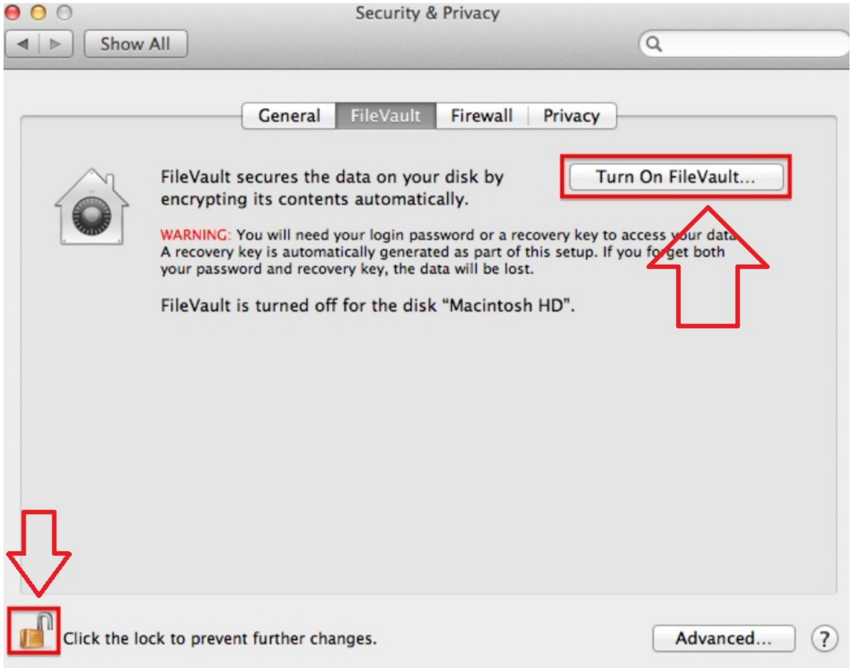
How to Enable Filevault on Apple Mac Computers

It is recommended to have at least OS X 10.7 or higher on your MAC, this has the current version of Filevault 2 which supports whole disk encryption.

If you have an older MAC which only supports 10.6 or older, this has Filevault 1, which only encrypts the home drive, not the whole disk.

Before enabling Filevault 2, it is important to make a full backup of your data. While the encryption process is generally simple and reliable, if something goes wrong, it is important to have a working back up.

Once all your data is securely backed up, log into the OS X with an account that has administrative privileges and go to **System Preferences > Security and Privacy > Filevault**. Click the padlock in the lower left of the window and enter your admin password in order to make changes, and then click on **Turn on Filevault**.



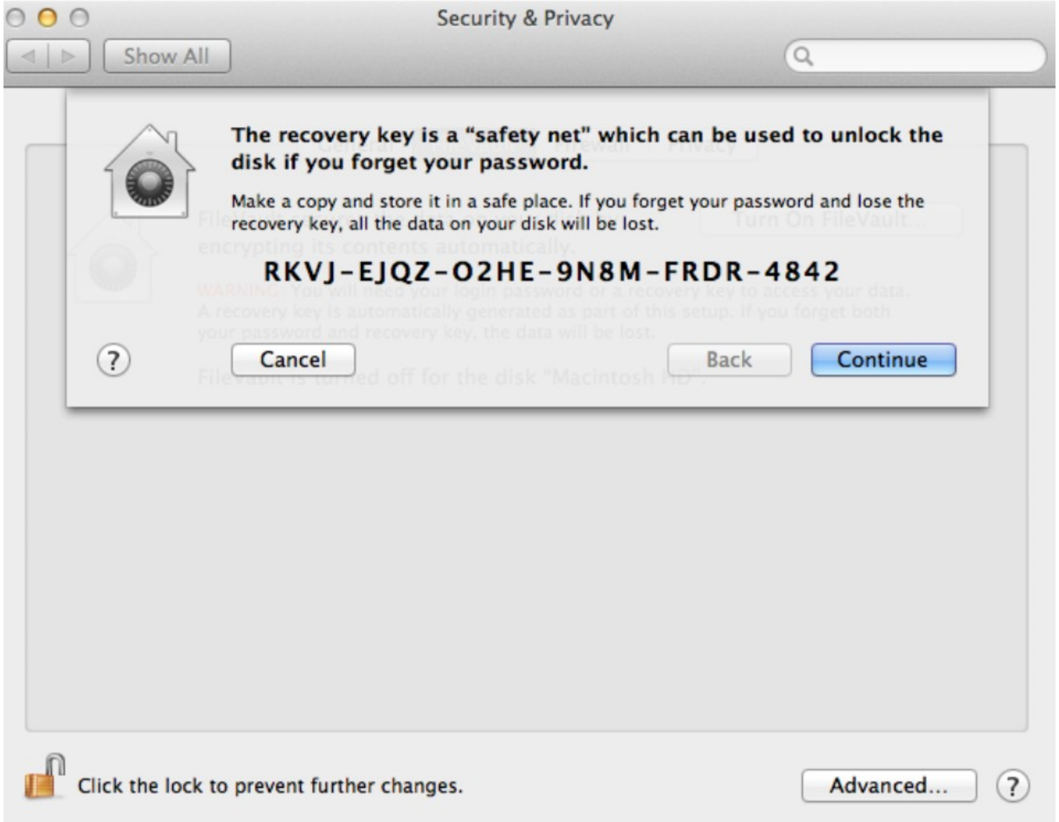
FileVault secures the data on your disk by encrypting its contents automatically.

WARNING: You will need your login password or a recovery key to access your data. A recovery key is automatically generated as part of this setup. If you forget both your password and recovery key, the data will be lost.

FileVault is turned off for the disk “Macintosh HD”.

Click the lock to prevent further changes.

FileVault 2 uses your existing account password so there is no need to set and remember a separate password to decrypt your drive. If you forget your password, a recovery key is generated as a backup so that you can still unlock your drive. This will be displayed only once, so keep a copy in a safe place.



The recovery key is a “safety net” which can be used to unlock the disk if you forget your password.

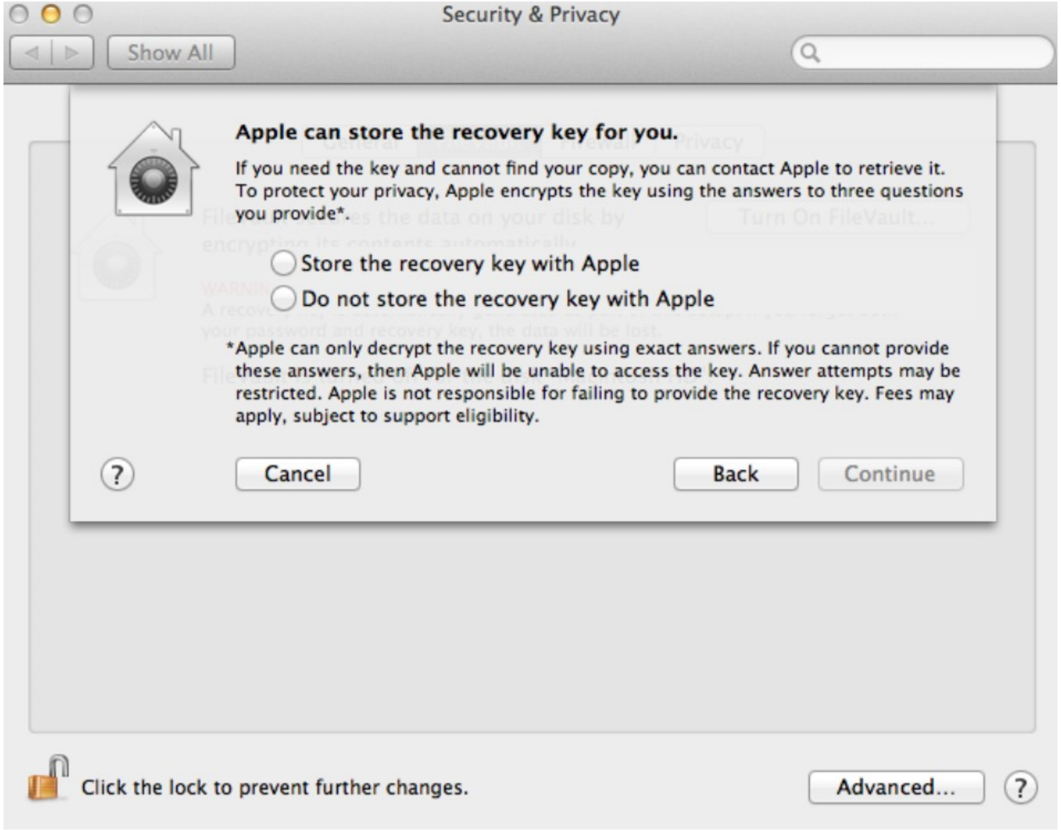
Make a copy and store it in a safe place. If you forget your password and lose the recovery key, all the data on your disk will be lost.

RKVJ-EJQZ-O2HE-9N8M-FRDR-4842

Click the lock to prevent further changes.

You have the option to store this key with Apple. To do so, just set the answers to three security questions when prompted.

Be aware, if you need to recover the key from Apple, they will charge you a fee to do this.



Apple can store the recovery key for you.

If you need the key and cannot find your copy, you can contact Apple to retrieve it. To protect your privacy, Apple encrypts the key using the answers to three questions you provide*.

○ Store the recovery key with Apple

○ Do not store the recovery key with Apple

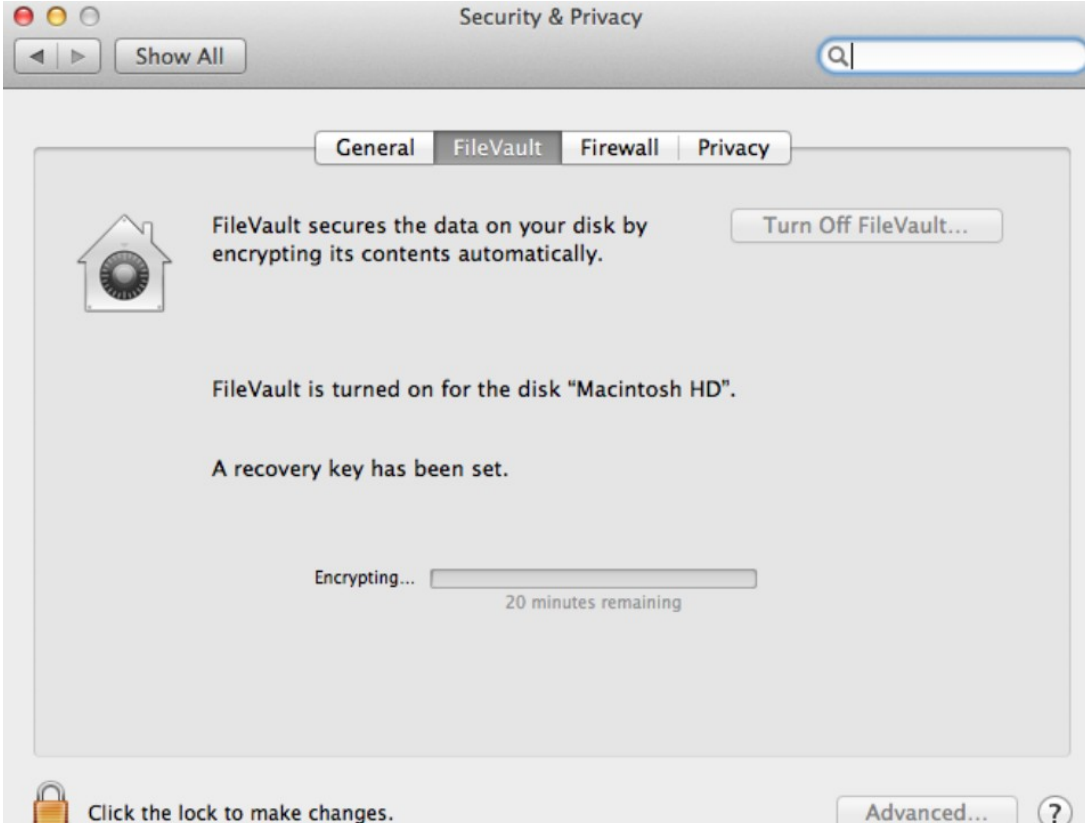
*Apple can only decrypt the recovery key using exact answers. If you cannot provide these answers, then Apple will be unable to access the key. Answer attempts may be restricted. Apple is not responsible for failing to provide the recovery key. Fees may apply, subject to support eligibility.

Click the lock to prevent further changes.

The computer will reboot and prompt you for your user account password at the EFI boot screen. If you have forgotten your password, click the question mark icon and you will be able to enter the recovery key. This process is how you will boot your Mac from now on with Filevault enabled.

Upon booting back into OS X immediately after enabling FileVault, you will notice it will take some time to encrypt your drive. You can follow the progress of this process from the same Filevault tab of the Security & Privacy preference pane that we mentioned above.

This initial encryption process only happens the first time, and will take between a few minutes to a few hours depending on the size of your drive and the speed of your Mac. You can continue to use your Mac during this process.



FileVault secures the data on your disk by encrypting its contents automatically.

FileVault is turned on for the disk “Macintosh HD”.

A recovery key has been set.

Encrypting…

20 minutes remaining

Click the lock to make changes.

Once the initial encryption is complete, so is the Filevault setup process. Your entire Mac system drive is now protected.

Best Practices

To ensure your laptop is secure, remember these best practices:

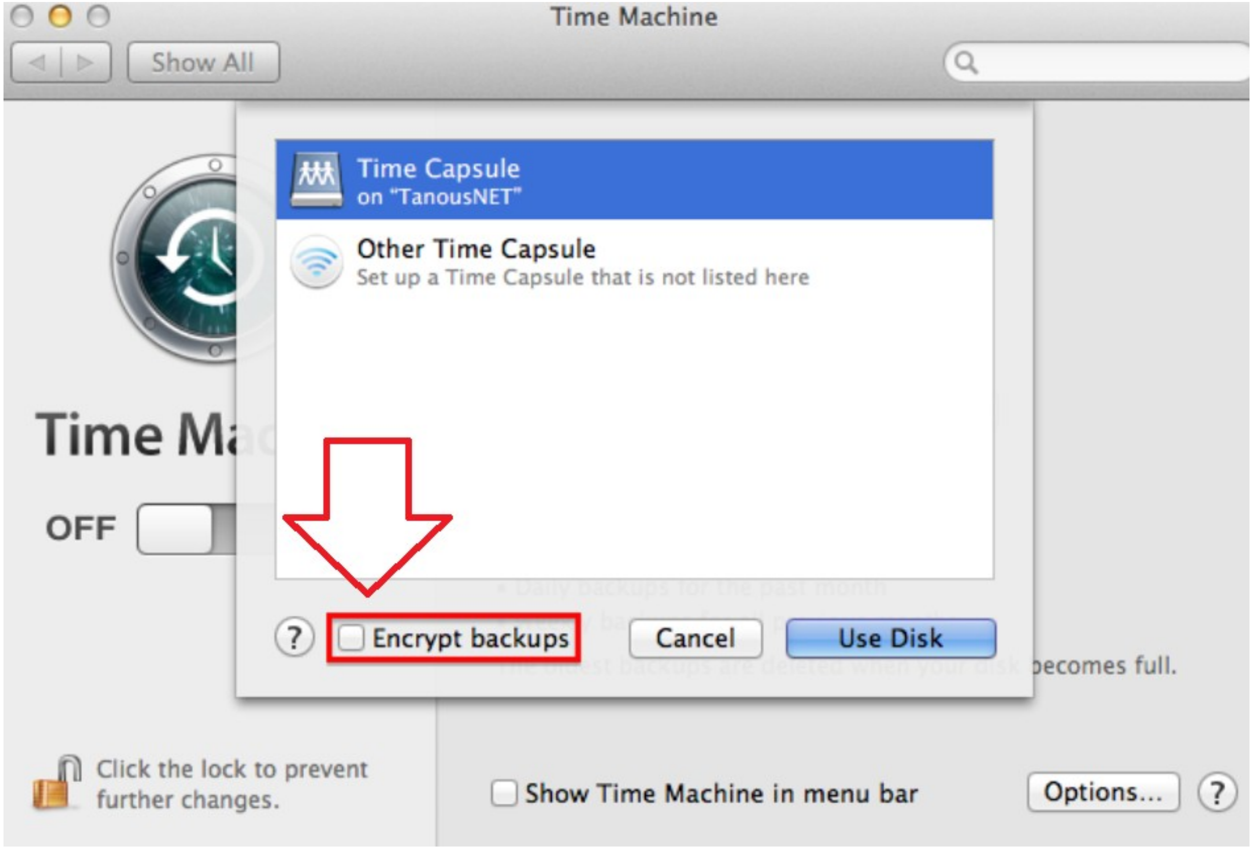
Do not leave your laptop unattended in any public location

Configure your Mac to require a password when waking from sleep or a screen saver (you can do this in **System Preferences>Security & Privacy>General**)

Fully power off the laptop if there is a chance of unauthorized access

Protecting your back ups:

Your Mac’s system drive may be encrypted, but your backups may be by default. If you are using Apple’s Time Machine, you can fix this by going to System Preferences > Time Machine > Select Disk, and checking the box Encrypt Backups. If you are using a third part backup solution, check to see if the software or service offers an option for encrypted backups.



For Mac with multiple user accounts, you can manage which users can unlock a FileVault-protected Mac.

If a Mac has multiple user accounts, you will be prompted to choose authorized users when first enabling FileVault in System Preferences. Click Enable User button and enter the user's password for each account you want to be able to boot and decrypt the Mac.

Note that while these users will be able to decrypt the entire system drive, the standard OS X user protections remain in place, meaning that one user will not be able to see another user's non-shared data from the Finder.