

DATA SECURITY PACKET

Revised June 2023



ENABLING BITLOCKER DRIVE ENCRYPTION ON WINDOWS 10

These instructions provide the procedure for turning on BitLocker Drive Encryption protection on an operating system drive of a computer with a TPM. After the drive is encrypted, the user logs on to the computer normally.

***NOTE* BitLocker is not available on Windows 10 Home Edition**

BitLocker Prerequisites

- You must be able to provide administrative credentials.
- You must be able to configure a printer if you want to print the recovery key.
- Your computer must meet BitLocker requirements (see below).

Enabling BitLocker for Windows 10

1. Click **Start**, type or click **Control Panel**, click **System and Security**, and then click **BitLocker Drive Encryption**. From there you will see whether BitLocker is On or Off. If it is on, you are encrypted. If it is Off, follow the steps below.
2. Click **Turn On BitLocker** for the operating system drive. BitLocker will scan your computer to make sure that it meets the BitLocker system requirements. If your computer meets the requirements, BitLocker will inform you of the next steps that need to be taken to turn on BitLocker, such as drive preparation, turning on the TPM, and encrypting the drive.

If your TPM is not initialized, the BitLocker setup wizard will instruct you to remove any CDs, DVDs, or USB drives from the computer and restart the computer to begin the process of turning on the TPM. You will either be prompted to enable the TPM before the operating system boots or in some cases you will need to navigate to the BIOS options and enable the TPM manually. This behavior depends on the BIOS of the computer. After you confirm that you want the TPM enabled, the operating system will start and the **Initializing the TPM security hardware** progress indicator will be displayed.

If your computer does not have a TPM, you can still use BitLocker, but you will be using the **Startup key only** authentication method. All of the required encryption key information is stored on a USB flash drive, which the user must insert into the computer during startup. The key stored on the USB flash drive unlocks the computer. Using a TPM is recommended because it helps protect against attacks made against the computer's critical startup process. To use this method, your computer must support the reading of USB devices in the pre-boot environment and you must enable this authentication method by selecting the check box **Allow BitLocker without a compatible TPM** in the Group Policy setting **Require additional authentication at startup**, which is located in the following location in the Local Group Policy Editor: Computer Configuration Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives.

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**.

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.

1. The BitLocker setup wizard asks if you are ready to encrypt the drive. Confirm that the **Run BitLocker system check box** is selected, and then click **Continue**.
2. Confirm that you want to restart the computer by clicking **Restart now**. The computer restarts, and BitLocker checks if the computer meets BitLocker requirements and is ready for encryption. If it is not, you will see an error message alerting you to the problem after you have logged on.
3. After the TPM is initialized, 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.
 - **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.

Warning

One of the items that BitLocker checks is the configuration of the system partition. BitLocker requires a minimum system partition size of 100 MB, and the Windows Recovery Environment requires 200 MB. When the operating system is installed, the system partition is automatically created by the setup process with a default size of 300 MB. However, this default partition size can be changed by computer manufacturers or system administrators when they install the operating system. If the system partition is exactly 100 MB, BitLocker setup assumes that you have a Windows Recovery DVD for use with your computer and the system check is completed without any errors. However, if you have a system partition size between 101 MB and 299 MB, the following error message will be displayed: "You will no longer be able to use Windows Recovery Environment unless it is manually enabled and moved to the system drive." If you have a Windows 10 DVD that contains the Windows Recovery Environment or you have another system recovery process in place, you may disregard this message and continue with BitLocker setup. Otherwise, you should check your system partition and verify that you have at least 200 MB of free space on your system partition so that the Windows Recovery Environment can be retained on the system drive along with the BitLocker Recovery Environment and other files that BitLocker requires to unlock the operating system drive.

4. If it is ready for encryption, the **Encrypting** status bar is displayed, which shows the progress of the drive encryption. You can monitor the ongoing completion status of the disk drive encryption by moving the mouse pointer over the BitLocker Drive Encryption icon in the notification area, at the far right of the taskbar. Encrypting the drive will take some time. You can use your computer during encryption, but performance might be slower. A completion message is displayed when encryption is finished.

By completing this procedure, you have encrypted the operating system drive and created a recovery key that is unique to this drive. The next time you log on, you will see no change. If the TPM ever changes or cannot be accessed, if there are changes to key system files, or if someone tries to start the computer from a disk to circumvent the operating system, the computer will switch to recovery mode and prevent Windows from starting.

WINDOWS COMPUTER SECURE USB/SD DEVICE ERASE



SDFormatter is installed on all Resident computers and on XenDesktop. To securely erase SD cards follow instructions below.

1. Open SDFormatter
2. Select your Drive: Be sure to select the correct drive. Once erased data cannot be recovered.
3. Click “Option”, change FORMAT TYPE to FULL (Erase), and click OK
4. Click “Format”

Note: This will securely format your device making all data unrecoverable and makes it writable.

MAC COMPUTER SECURE USB/SD DEVICE ERASE




1. Click on the **Applications** folder, then the **Utilities** folder and choose **Disk Utility**.
2. Select the USB/SD drive you want to erase from the list in the left panel.
3. Click the **Erase** category button on the top of the right panel.
4. Click the **Security Option** button.
5. Select “7-Pass Erase” for Secure Erase Options:
6. Click **OK** once selected.
7. Click **Erase**. Do not click "Erase Free Space" as this will not remove any data from the USB/SD device.
8. At the confirmation window, click **Erase** to start the erasure process.
9. A progress bar will appear in the lower right corner of the Disk Utility window with an estimated time for the erase process to complete. This may be several hours.
10. When erasure is finished, click the **Disk Utility** menu at the top, and choose **Quit Disk Utility**.
11. The USB/SD device should now be erased and ready for new use.

ENCRYPTING YOUR HOME FOLDER WITH FILEVAULT ON MAC OS X



To set up FileVault, you must be an administrator. When you encrypt your information using FileVault, a recovery key is created as a safeguard. If you forget your login password, you can use the recovery key to unlock the encoded contents. The recovery key should not be physically stored with your Mac where it can be discovered.

WARNING: Don't forget your recovery key. If you turn on FileVault and then forget your login password and cannot reset it, and you also forget your recovery key, you won't be able to log in and your files and settings will be lost forever.

1. Choose Apple menu > System Preferences, click Security & Privacy, then click FileVault.
2. Click the lock icon  to unlock it, then enter an administrator name and password.
3. Click Turn On FileVault.
4. If your Mac has multiple users, a list of users appears. You can allow users to log in after the Mac starts up. If you don't, an administrator must log in before the user does.
5. For each user you want to enable, click Enable User, enter (or have the user enter) the user's login password, then click OK.
6. If the recovery key is hidden, click the triangle next to Show Recovery Key.
7. Copy the recovery key and store it in a safe place, then click Continue.
8. Choose whether you want the added safeguard of storing the recovery key with Apple.
9. Choose "Do not store the recovery key with Apple." and bring to recovery key to Dental Informatics for safe keeping.
10. Click Continue.
11. Click Restart.
12. After you restart, encryption begins. It may take some time to encrypt your information, depending on how much is stored. However you can use your Mac as usual while your information is being encrypted.



ENABLING DATA PROTECTION ON AN IOS DEVICE

About iOS Encryption

Data protection is a feature available for devices that offer hardware encryption, including iPhone 3GS and later, all iPad models, and iPod touch (3rd generation and later). This article outlines how to enable and verify data protection.

iOS Products Affected

All Apple mobile devices to include iPad, iPod, iPod Touch, and iPhone.

Data protection enhances the built-in hardware encryption by protecting the hardware encryption keys with your passcode. This provides an additional layer of protection for your email messages and attachments

Enable data protection by configuring a passcode for your device:

1. Tap Settings > Touch ID and Passcode > Passcode Lock.
2. Follow the prompts to create a passcode.
3. After the passcode is set, scroll down to the bottom of the screen and verify that the text "Data protection is enabled" is visible.

Passcode Tips

Use these passcode settings to maximize passcode security:

- Set Require Passcode to Immediately.
- Disable Simple Passcode to allow the use of longer, alphanumeric, passcodes.
- Enable Erase Data to automatically erase the device after ten failed passcode attempts.

CONFIGURING “FIND MY IPHONE”



If you misplace your iPhone, iPad, iPod touch, or Mac, the Find My iPhone app will let you use another iOS device to find it and protect your data. Simply install this free app on another iOS device, open it, and sign in with your Apple ID. Find My iPhone will help you locate your missing device on a map. You can then choose to display a message or play a sound, remotely lock your device, or erase your data on it.

To see all your devices in Find My iPhone, use the same *Apple ID* when you set up each device.

Set up an iOS device

1. On your device’s Home screen, tap Settings, then tap iCloud.

If you’re asked to sign in, enter your *Apple ID*. If you don’t have one, tap Create a new Apple ID, then follow the instructions.

2. If Find My iPhone (or Find My iPad or Find My iPod) is turned off, tap Find My iPhone, then tap to turn it on.
3. Tap to turn on Send Last Location.

If your device is lost or stolen and its battery charge level becomes critically low, its location is sent to Apple automatically. When you use Find My iPhone to locate that device, you see where it was before its battery ran out of charge.

For added security, set up a passcode that needs to be entered before anyone can access the apps and information on your device. To set up a passcode, go to Settings > Passcode or Touch ID & Passcode. If your device has iOS 5, iOS 10 or later, Touch ID + Passcode.

Set up a Mac

1. On your Mac, choose Apple menu > System Preferences, then click iCloud.

If you’re asked to sign in, enter your *Apple ID*. If you don’t have one, click Create new Apple ID, then follow the instructions.

2. If Find My Mac is turned off, select it to turn it on.

For added security, make sure your user account requires a password and that automatic login is turned off in Users & Groups preferences.



ENABLING DATA PROTECTION ON AN ANDROID DEVICE

Enabling Encryption for Android

Each manufacturer's menu layout may be different. Below we reference stock Android.

Note: Enabling the PIN or PASSWORD lock screen will by default enable device encryption on your Android device.

Configure Your Lock Screen

1. Go to the **Settings menu** on your device
2. Scroll down "Security" or "Security and Screen Lock" or "Lock Scree"
3. Enter the "Lock Screen" menu and select "Screen Lock" under "Screen Security"
4. Select either PIN or PASSWORD and configure