Enabling BitLocker Drive Encryption on Windows 7

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.

Before you start

To complete the procedure in this scenario:

- 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.

To turn on BitLocker Drive Encryption on an operating system drive

1. Click **Start**, click **Control Panel**, click **System and Security**, and then click **BitLocker Drive Encryption**.
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 you have a single partition for your operating system drive, BitLocker will prepare the drive by shrinking the operating system drive and creating a new system partition to use for system files that are required to start or recover the operating system and that cannot be encrypted. This drive will not have a drive letter to help prevent the storing of data files on this drive inadvertently. After the drive is prepared, the computer must be restarted.

   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. Using the **Startup key only** method only encrypts the drive; it does not provide any validation of the early boot components or hardware tampering. To use this method, your computer must support the reading of USB devices in the preboot 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**.
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.

   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.

4. The BitLocker setup wizard asks if you are ready to encrypt the drive. Confirm that the **Run BitLocker system check** check box is selected, and then click **Continue**.
5. 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.

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 7 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

6. 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.