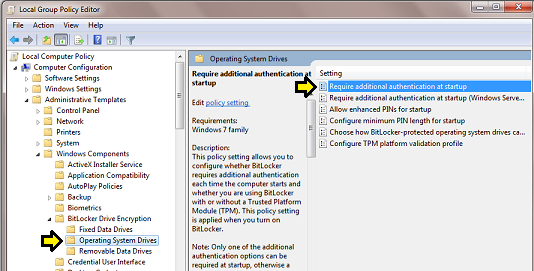
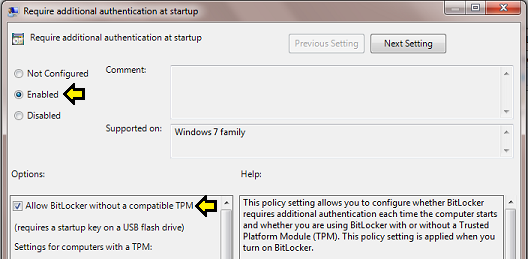
You will need to adjust the *Group Policy* on the machine. Click *Start* or tap the Windows key and type *gpedit.msc* then hit *Enter*. This should open the *Local Group Policy Editor*.



Use the left pane to navigate to Computer Configuration ► Administrative Templates ► Windows Components ► Bit Locker Drive Encryption ► Operating System Drives then double-click on the *Require additional authentication at startup* option in the right pane.



First choose *Enabled* for this policy option then check *Allow BitLocker without a compatible TPM*. Be sure that you read and understand the caveats and conditions explained in the right *Help* pane. Know that you will need a USB *key* to use this alternative method of BitLocker security.

*"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 a USB drive is required for start-up and 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 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 authentication methods can be used at startup to provide added protection for encrypted data. When the computer starts, it can use only the TPM for authentication, or it can also require insertion of a USB flash drive containing a startup key, the entry of a 4-digit to 20-digit personal identification number (PIN), or both.*  
  
*If you enable this policy setting, users can configure advanced startup options in the BitLocker setup wizard.*  
  
*If you disable or do not configure this policy setting, users can configure only basic options on computers with a TPM.*  
  
*Note: If you want to require the use of a startup PIN and a USB flash drive, you must configure BitLocker settings using the command-line tool manage-bde instead of the BitLocker Drive Encryption setup wizard."*

When you are satisfied that you have all of the conditions understood, click *OK* to change this group policy option. Restart the machine before attempting to configure BitLocker on a drive. Make sure you have an appropriate USB device to use as a *key* before starting the BitLocker configuration.