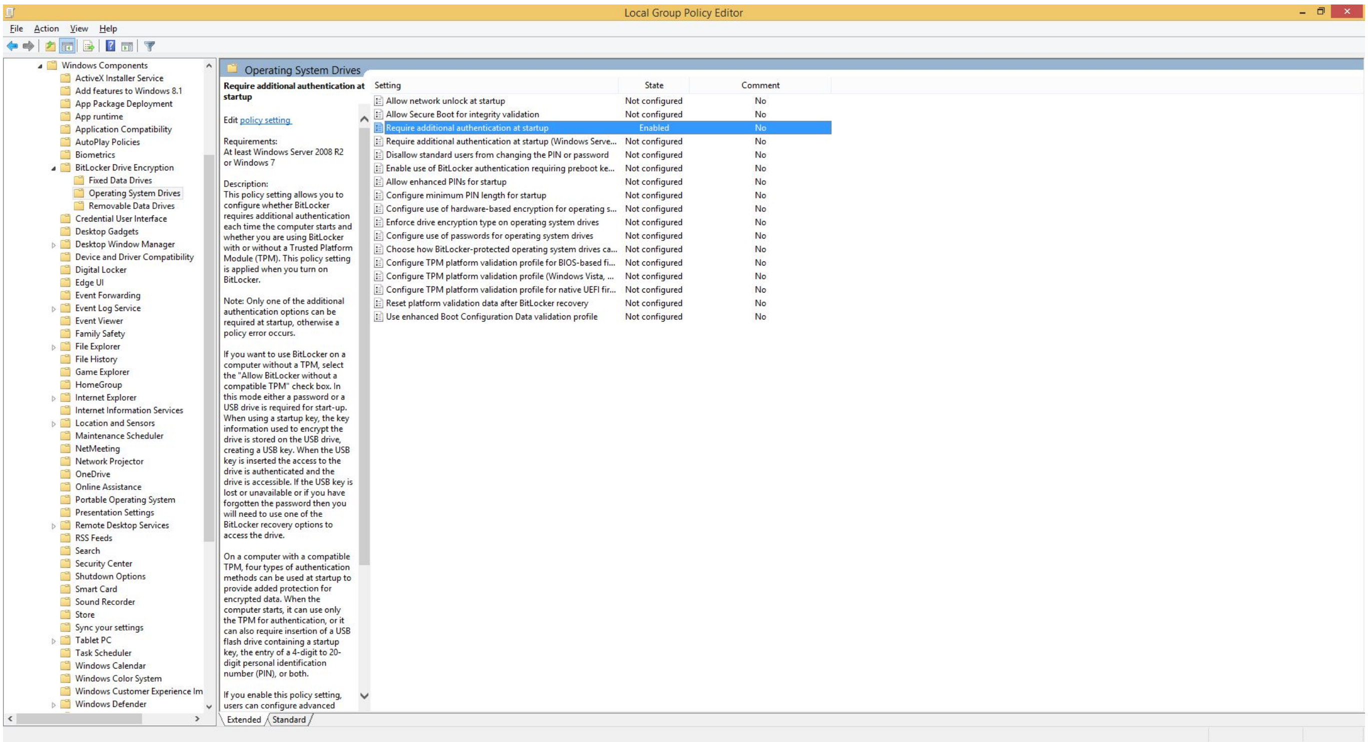
BitLocker: Lock drives w/o TPM device

“Nay!” they say; “It's not possible!” they say; “You can't lock a drive with BitLocker without a TPM device!” they say… “Bah!” I say, what a load of “#$%*&! That said (pun intended) do read on and find out a simple way to encrypt that which matters most and get away with it without the use of “training wheels”.

A great honor has been bestowed upon You (yes - YOU) to personally deliver Granny's latest highly classified chocolate chip and mozzarella muffin formula to the cookie factory and to do that you have been handed a cuff-to-wrist-to-special-titanium-alloy-cloaked-by-light-reflecting-quantum-piezo-oled-ccd-sensor-grenade-proof-uber-light-water-tight-non-smoking-iPhone-compatible-gps-traceable laptop case that contains the notebook PC on which's HDD the recipe is stored. But You know better then to trust just another stylish carry case and a logon screen so You decide to up the security ante and encrypt the said hard drive using integrated Windows BitLocker technology. And so after 26h 37m and 04s that has taken You to insert the special 6548792134897456321-bit encrypted password (and swipe all twenty fingers through the scanner + provide a not more then 15 minutes old urine sample to boot) and finally get the darn thing open, sadly You find out that Your cunning plan to additionally enhance security goes out the window 'cause some knucklehead forgot to buy a model that actually HAS a TPM chip! Never fear - Dr. Vlad is here! ;)

All You need to do is as simple as quickly climbing up a tree whilst being chased by a drunk Mogwai smoking three cigarettes at the same time:

Open up Local Group Policy Editor running the gpedit.msc cmdlet and go to: Administrative Templates → Windows Components → BitLocker Drive Encryption → Operating System Drives



Require additional authentication at startup

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.

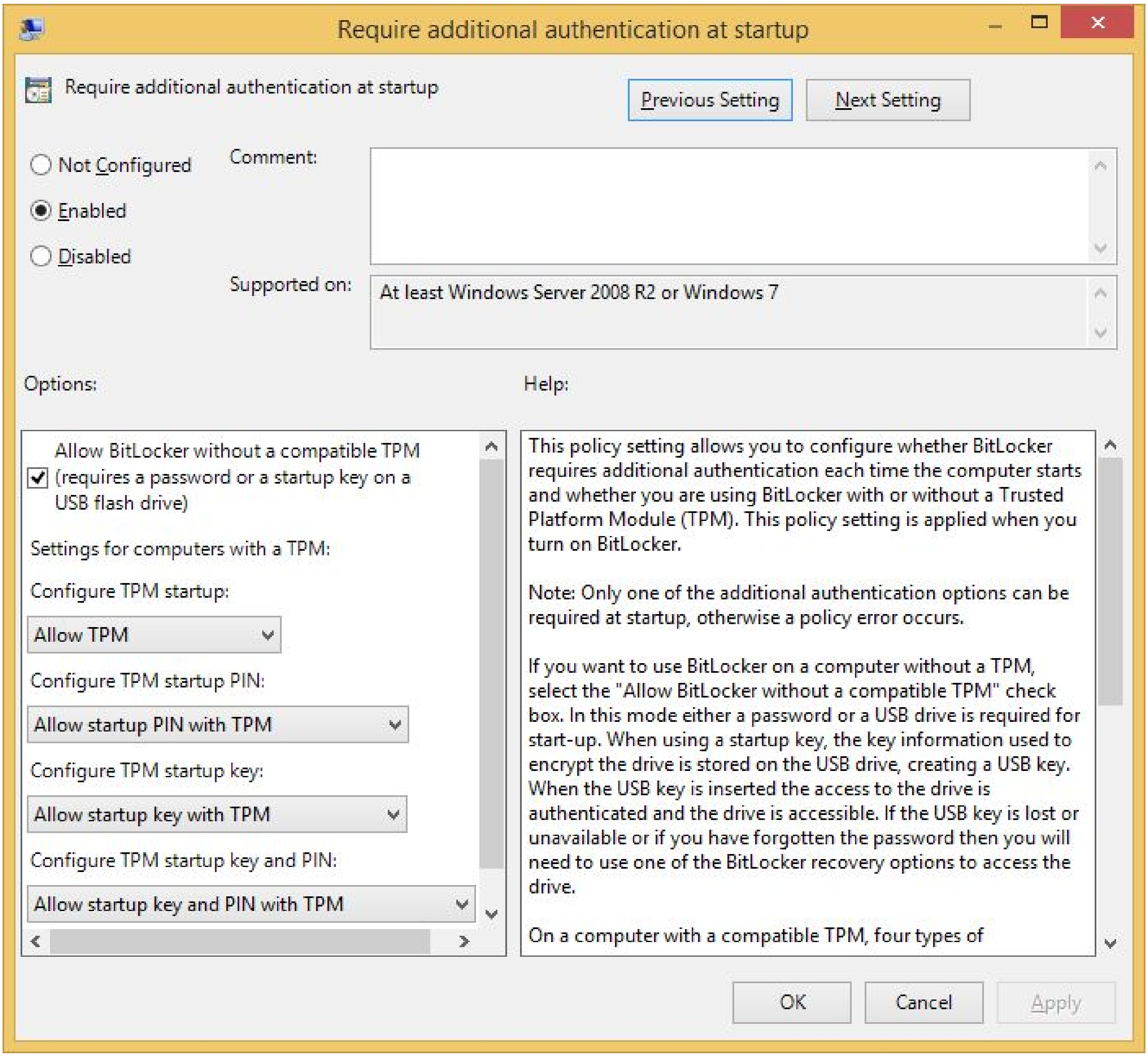
If you want to use BitLocker on a computer without a TPM, select the "Allow BitLocker without a compatible TPM" check box. In this mode either a password or a USB drive is required for start-up. When using a startup key, the key information used to encrypt the drive is stored on the USB drive, creating 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 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

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	Enabled	No
Require additional authentication at startup (Windows Serve...	Not configured	No
Disallow standard users from changing the PIN or password	Not configured	No
Enable use of BitLocker authentication requiring preboot ke...	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 for operating s...	Not configured	No
Enforce drive encryption type on operating system drives	Not configured	No
Configure use of passwords for operating system drives	Not configured	No
Choose how BitLocker-protected operating system drives ca...	Not configured	No
Configure TPM platform validation profile for BIOS-based fi...	Not configured	No
Configure TPM platform validation profile (Windows Vista, ...	Not configured	No
Configure TPM platform validation profile for native UEFI fir...	Not configured	No
Reset platform validation data after BitLocker recovery	Not configured	No
Use enhanced Boot Configuration Data validation profile	Not configured	No

Enable the policy: “Require additional authentication at startup” and be sure that the “Allow BitLocker without a compatible TPM” option check box is ticked.



Require additional authentication at startup

Require additional authentication at startup

○ 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

All done!

Now go and finally get that recipe to the factory! Production is at a halt while Yo're fiddling about with some IT nonsense thinking You're 007, and all that THAT is going to achieve is make Granny send You of to bed without any milk and cookies :P

From:
https://wiki.plecko.hr/ - **Eureka Moment**

Permanent link:
https://wiki.plecko.hr/doku.php?id=windows:misc:bitlocker_no_tpm

Last update: **2019/10/31 09:06**