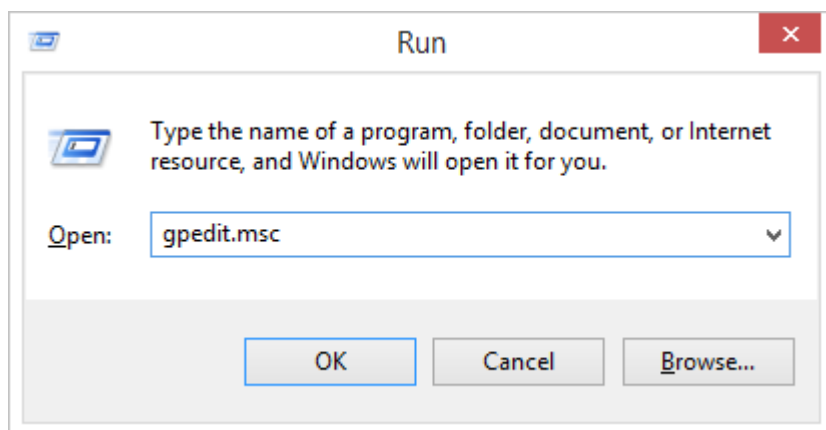


# Bitlocker: Enable PIN on boot

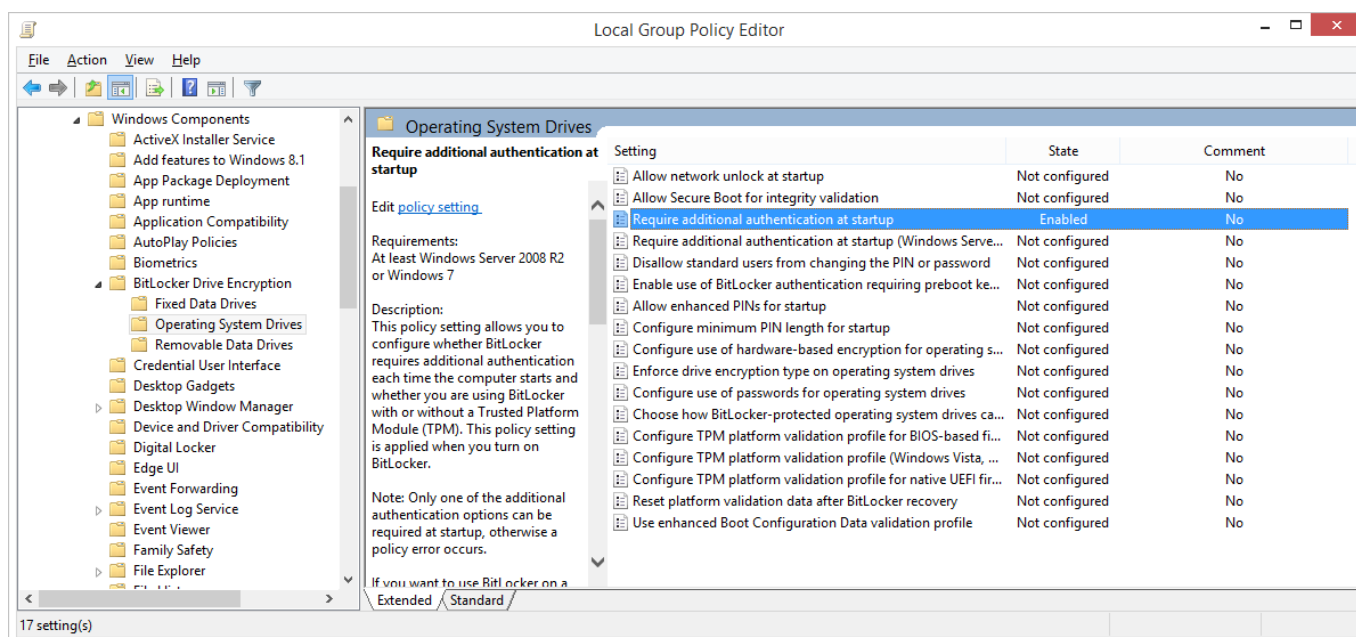
If you want your system to require a PIN number in order to unlock a Bitlocker encrypted drive at boot time, you need to change one small GPO setting (assuming that you have Bitlocker already set up):

Start Group Policy editor by pressing Windows+R and entering the command 'gpedit.msc'



Start the Local Group Policy Editor

Navigate to Local Computer Policy → Computer Configuration → Administrative Templates → Windows Components → Bitlocker Drive Encryption → Operating System Drives



Navigate to 'Operating System Drives'

Select the 'Require additional authentication at startup' option, and set it to 'Enabled'. Then set 'Configure TPM startup PIN' to 'Require startup PIN with TPM'

Require additional authentication at startup

Require additional authentication at startup

Previous Setting Next Setting

☐ Not Configured Comment:

☒ Enabled

☐ Disabled

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

Options:

Help:

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:  
Require 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

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

OK Cancel Apply

Set 'Configure TPM startup pin' to 'Require startup PIN with TPM'

Now open CMD in elevated mode and enter the command to set the PIN

```
manage-bde -protectors -add c: -TPMAndPIN
```

This will prompt you for a PIN which You will enter at Boot time.

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

Permanent link:  
[https://wiki.plecko.hr/doku.php?id=windows:client\\_os:pin\\_on\\_boot](https://wiki.plecko.hr/doku.php?id=windows:client_os:pin_on_boot)

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

