

How to Enable a Pre-Boot BitLocker PIN on Windows

Step One: Enable BitLocker (If You Haven't Already)



RELATED: [How to Set Up BitLocker Encryption on Windows](#)

This is a BitLocker feature, so you have to use BitLocker encryption to set a pre-boot PIN. This is only available on Professional and Enterprise editions of Windows. Before you can set a PIN, you have to [enable BitLocker for your system drive](#).

Note that, if you go out of your way to [enable BitLocker on a computer without a TPM](#), you'll be prompted to create a startup password that's used instead of the TPM. The below steps are only necessary when enabling BitLocker on computers with TPMs, which [most modern computers have](#).

If you have a Home version of Windows, you won't be able to use BitLocker. You may have the [Device Encryption](#) feature instead, but this works differently from BitLocker and doesn't allow you to provide a startup key.

Step Two: Enable the Startup PIN in Group Policy Editor

Once you've enabled BitLocker, you'll need to go out of your way to enable a PIN with it. This requires a Group Policy settings change. To open the Group Policy Editor, press Windows+R, type

“gpedit.msc” into the Run dialog, and press Enter.

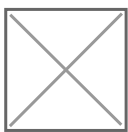
ADVERTISEMENT

Head to Computer Configuration > Administrative Templates > Windows Components > BitLocker Drive Encryption > Operating System Drives in the Group Policy window.

Double-click the “Require Additional Authentication at Startup” Option in the right pane.



Select “Enabled” at the top of the window here. Then, click the box under “Configure TPM Startup PIN” and select the “Require Startup PIN With TPM” option. Click “OK” to save your changes.



Step Three: Add a PIN to Your Drive

You can now use the `manage-bde` command to add the PIN to your BitLocker-encrypted drive.

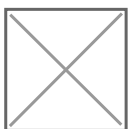
To do this, launch a Command Prompt window as Administrator. On Windows 10 or 8, right-click the Start button and select “Command Prompt (Admin)”. On Windows 7, find the “Command Prompt” shortcut in the Start menu, right-click it, and select “Run as Administrator”

ADVERTISEMENT

Run the following command. The below command works on your C: drive, so if you want to require a startup key for another drive, enter its drive letter instead of `c:` .

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

You’ll be prompted to enter your PIN here. The next time you boot, you’ll be asked for this PIN.



To double-check whether the TPMAndPIN protector was added, you can run the following command:

```
manage-bde -status
```

(The “Numerical Password” key protector displayed here is your recovery key.)



How to Change Your BitLocker PIN

To change the PIN in the future, open a Command Prompt window as Administrator and run the following command:

```
manage-bde -changePIN c:
```

You'll need to type and confirm your new PIN before continuing.



How to Remove the PIN Requirement

If you change your mind and want to stop using the PIN later, you can undo this change.

ADVERTISEMENT

First, you'll need to head to the Group Policy window and change the option back to “Allow Startup PIN With TPM”. You can't leave the option set to “Require Startup PIN With TPM” or Windows won't allow you to remove the PIN.



Next, open a Command Prompt window as Administrator and run the following command:

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

This will replace the “TPMandPIN” requirement with a “TPM” requirement, deleting the PIN. Your BitLocker drive will automatically unlock via your computer’s TPM when you boot.



To check that this completed successfully, run the status command again:

```
manage-bde -status c:
```



If you forget the PIN, you’ll need to provide the BitLocker recovery code you should have saved somewhere safe when you enabled BitLocker for your system drive.

Revision #1

Created 2021-07-13 16:33:49 UTC by batezippi

Updated 2021-07-13 16:34:38 UTC by batezippi