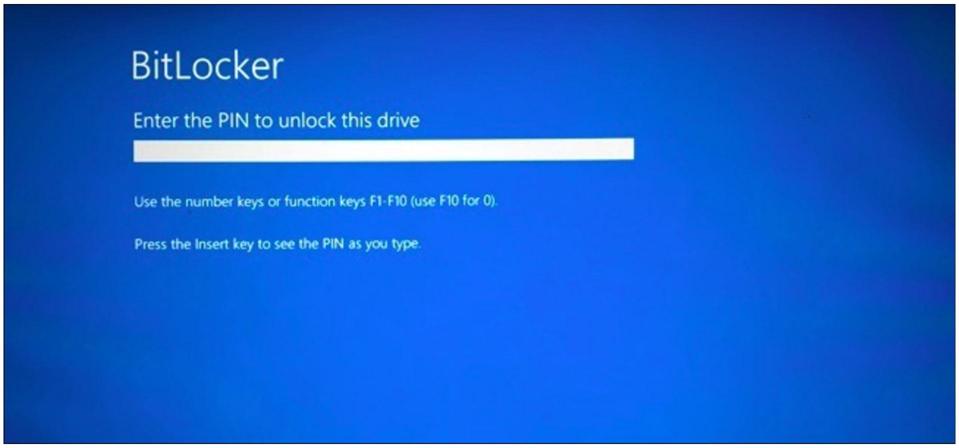
How-To Geek

How to Enable a Pre-Boot BitLocker PIN on Windows

CHRIS HOFFMAN @chrisbhoffman
UPDATED JUL 6, 2017, 8:58 PM EST | 3 MIN READ



BitLocker

Enter the PIN to unlock this drive

Use the number keys or function keys F1-F10 (use F10 for 0).

Press the Insert key to see the PIN as you type.

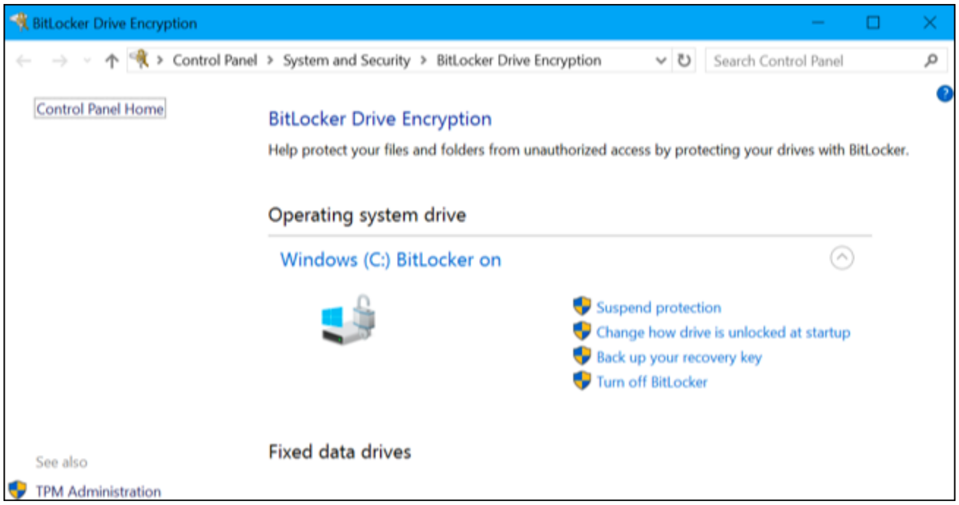
If you encrypt your Windows system drive with BitLocker, you can add a PIN for additional security. You'll need to enter the PIN each time you turn on your PC, before Windows will even start. This is separate from a login PIN, which you enter after Windows boots up.

RELATED: ***How to Use a USB Key to Unlock a BitLocker-Encrypted PC***

A pre-boot PIN prevents the encryption key from automatically being loaded into system memory during the boot process, which protects against direct memory access (DMA) attacks on systems with hardware vulnerable to them. Microsoft's documentation explains this in more detail.

Step One: Enable BitLocker (If You

Haven’t Already)


BitLocker Drive Encryption
Control Panel > System and Security > BitLocker Drive Encryption
Search Control Panel
Control Panel Home
See also
TPM Administration

BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

Operating system drive

Windows (C:) BitLocker on

Suspend protection
Change how drive is unlocked at startup
Back up your recovery key
Turn off BitLocker

Fixed data drives

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.

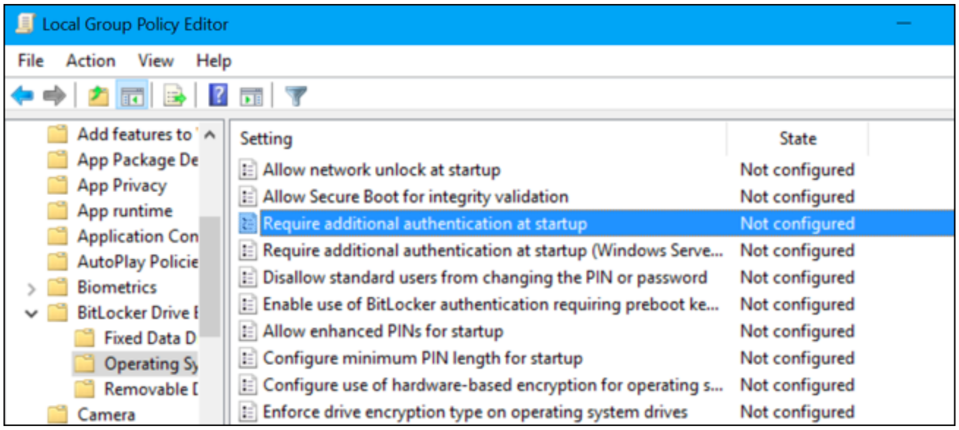
If you have a Home version of Windows, you won’t be able to use BitLocker. You may have the Device Encryption feature instead, but this works differently from BitLocker and doesn’t allow you to provide a startup key.

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.

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.



Setting	State
Allow network unlock at startup	Not configured
Allow Secure Boot for integrity validation	Not configured
Require additional authentication at startup	Not configured
Require additional authentication at startup (Windows Serve...	Not configured
Disallow standard users from changing the PIN or password	Not configured
Enable use of BitLocker authentication requiring preboot ke...	Not configured
Allow enhanced PINs for startup	Not configured
Configure minimum PIN length for startup	Not configured
Configure use of hardware-based encryption for operating s...	Not configured
Enforce drive encryption type on operating system drives	Not configured

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.

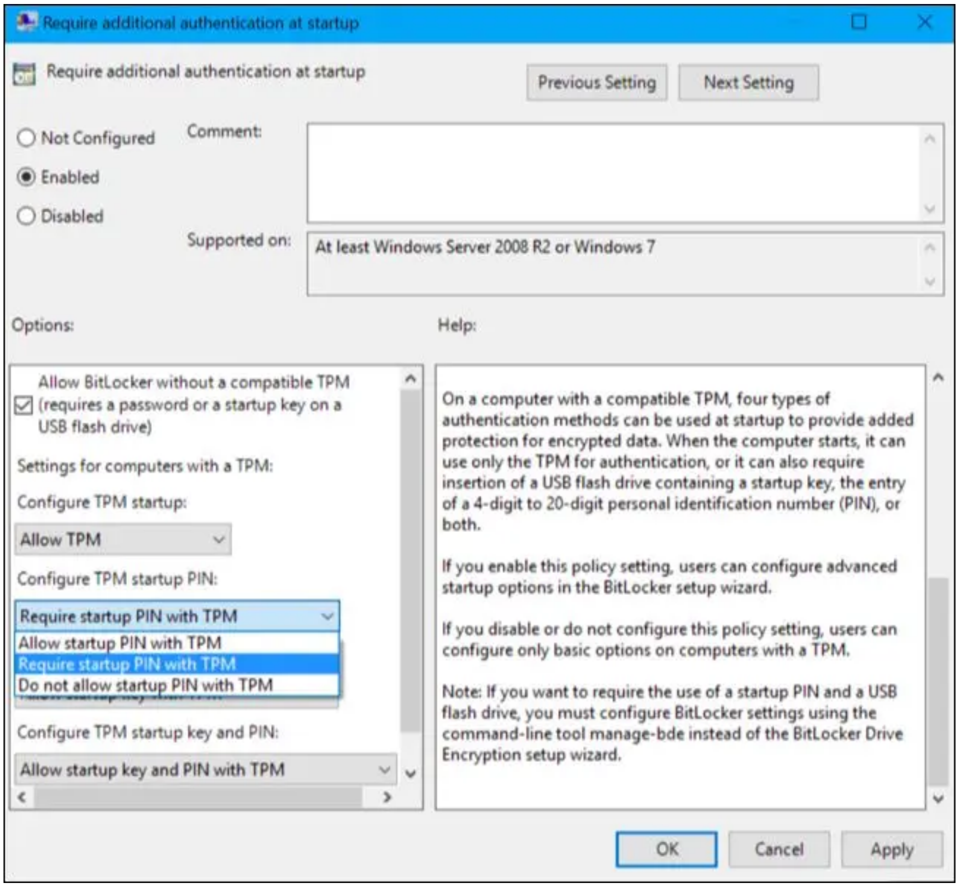
THE BEST TECH NEWSLETTER ANYWHERE

Join **425,000** subscribers and get a daily digest of features, articles, news, and trivia.

e-mail address

Sign Me Up!

By submitting your email, you agree to the Terms of Use and Privacy Policy.



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: Require startup PIN with TPM

- Allow startup PIN with TPM
- Require startup PIN with TPM
- Do not allow startup PIN with TPM

Configure TPM startup key and PIN: Allow startup key and PIN with TPM

Help:

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.

Step Three: Add a PIN to Your Drive

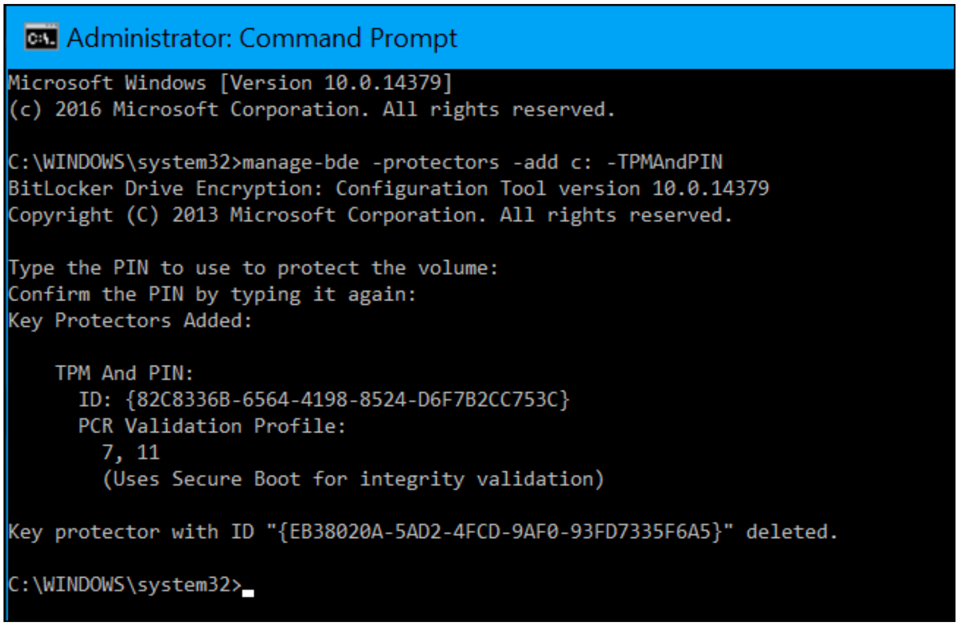
You can now use the `manage-bde` command to add the PIN to your BitLocker-encrypted drive.

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”

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.

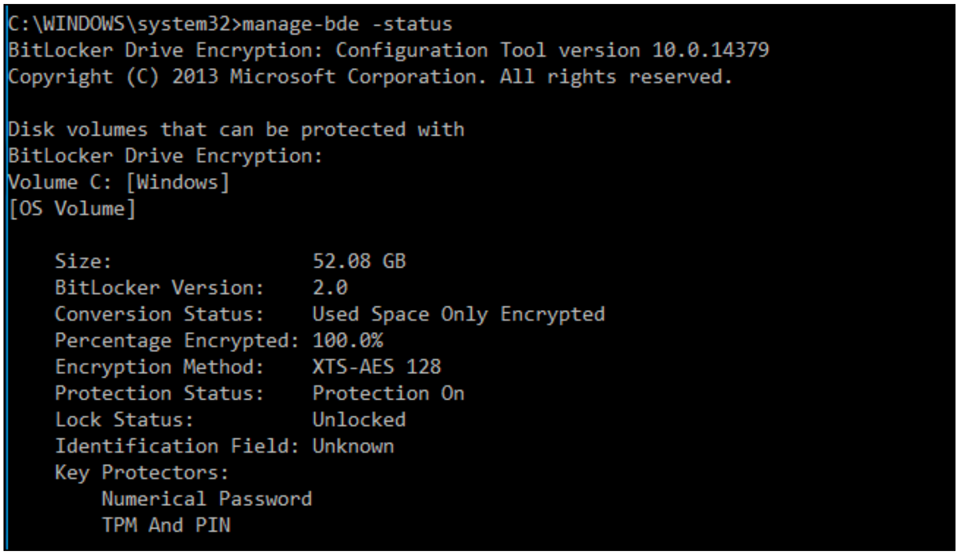


```
Microsoft Windows [Version 10.0.14379]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>manage-bde -protectors -add c: -TPMAndPIN
BitLocker Drive Encryption: Configuration Tool version 10.0.14379
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

Type the PIN to use to protect the volume:
Confirm the PIN by typing it again:
Key Protectors Added:

    TPM And PIN:
      ID: {82C8336B-6564-4198-8524-D6F7B2CC753C}
      PCR Validation Profile:
        7, 11
        (Uses Secure Boot for integrity validation)

Key protector with ID "{EB38020A-5AD2-4FCD-9AF0-93FD7335F6A5}" deleted.

C:\WINDOWS\system32>
```

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.)



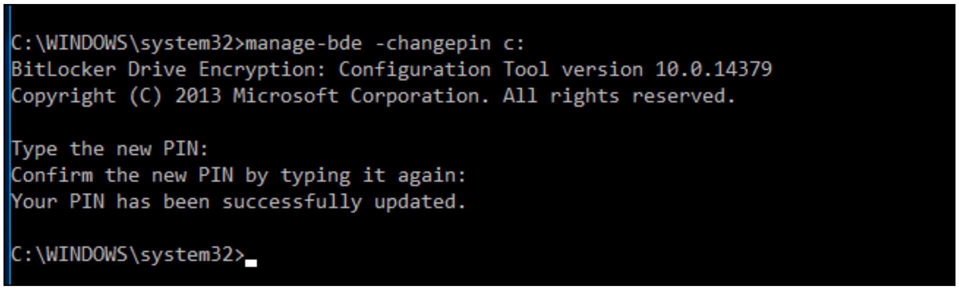
```
C:\WINDOWS\system32>manage-bde -status
BitLocker Drive Encryption: Configuration Tool version 10.0.14379
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

Disk volumes that can be protected with
BitLocker Drive Encryption:
Volume C: [Windows]
[OS Volume]

    Size:                 52.08 GB
    BitLocker Version:    2.0
    Conversion Status:    Used Space Only Encrypted
    Percentage Encrypted: 100.0%
    Encryption Method:    XTS-AES 128
    Protection Status:    Protection On
    Lock Status:          Unlocked
    Identification Field: Unknown
    Key Protectors:
        Numerical Password
        TPM And PIN
```

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.

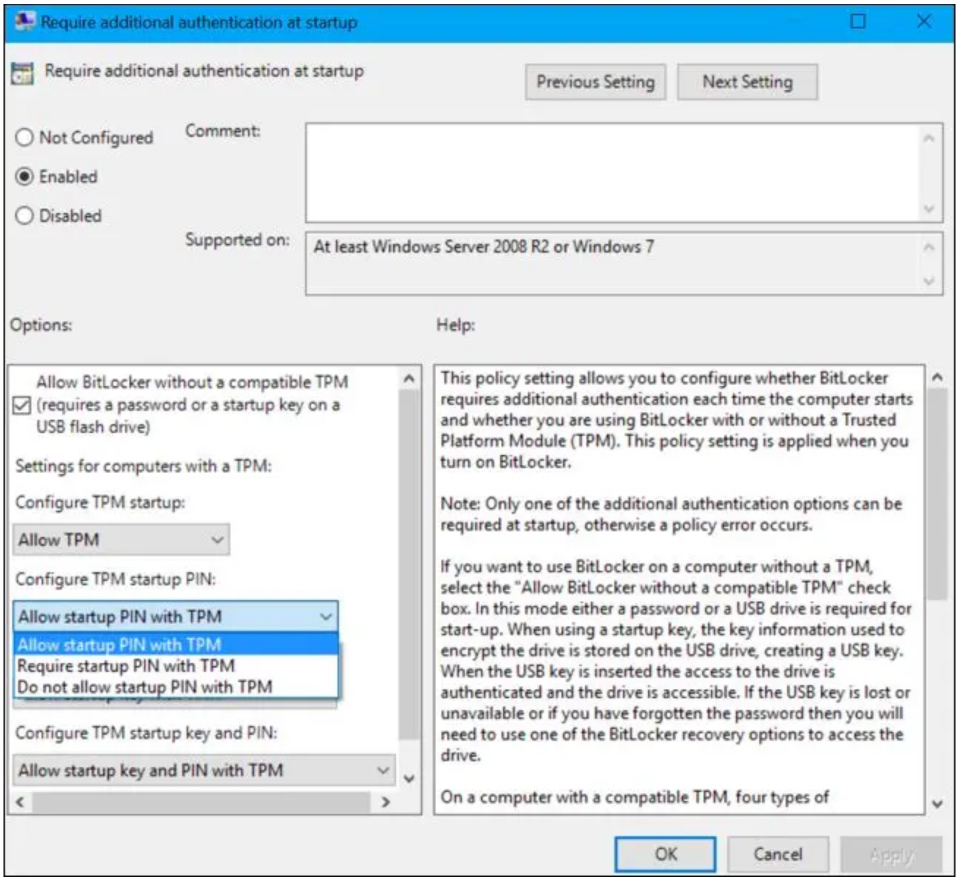


```
C:\WINDOWS\system32>manage-bde -changepin c:
BitLocker Drive Encryption: Configuration Tool version 10.0.14379
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

Type the new PIN:
Confirm the new PIN by typing it again:
Your PIN has been successfully updated.

C:\WINDOWS\system32>_
```

How to Remove the PIN Requirement

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

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.


Require additional authentication at startup
Require additional authentication at startup
Previous Setting
Next Setting
Comment:
Supported on:
Options:
Help:
OK
Cancel
Apply

○ Not Configured
● Enabled
○ Disabled

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

☑ 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

- Allow startup PIN with TPM
- Require startup PIN with TPM
- Do not allow startup PIN 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.

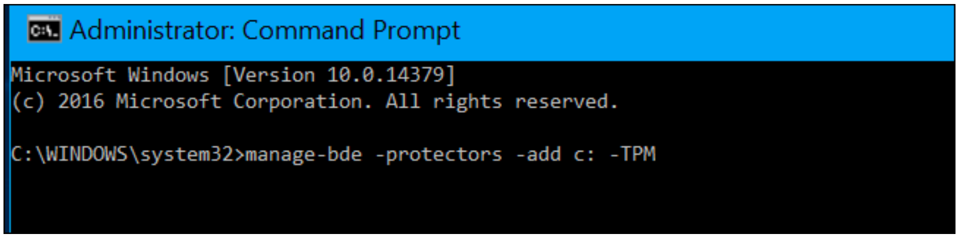
If you want to use BitLocker on a computer without a TPM, select the "Allow BitLocker without a compatible TPM" check box. In this mode either a password or a USB drive is required for start-up. When using a startup key, the key information used to encrypt the drive is stored on the USB drive, creating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

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

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

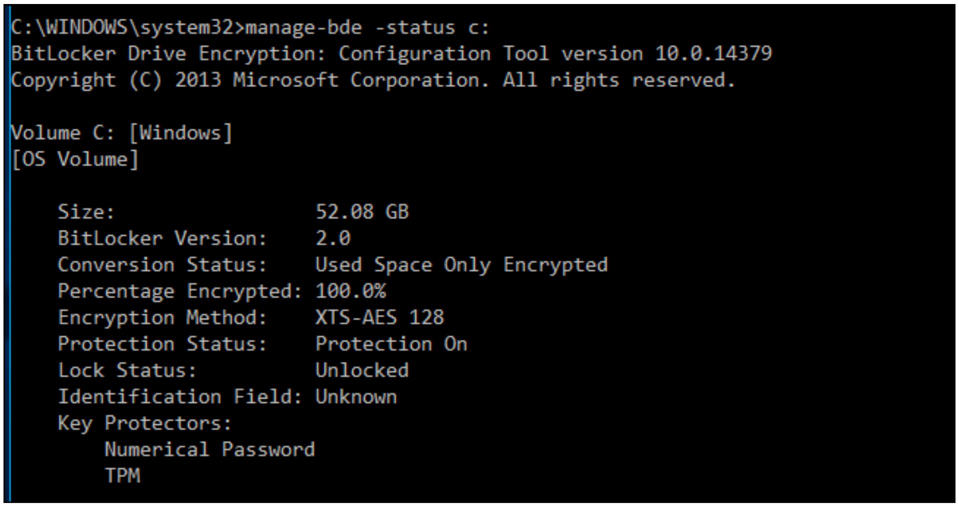
This will replace the “TPMandPIN” requirement with a “TPM” requirement, deleting the PIN. Your BitLocker drive will automatically unlock via your computer’s TPM when you boot.



```
Microsoft Windows [Version 10.0.14379]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>manage-bde -protectors -add c: -TPM
```

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

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



```
C:\WINDOWS\system32>manage-bde -status c:
BitLocker Drive Encryption: Configuration Tool version 10.0.14379
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

Volume C: [Windows]
[OS Volume]

    Size:                 52.08 GB
    BitLocker Version:    2.0
    Conversion Status:    Used Space Only Encrypted
    Percentage Encrypted: 100.0%
    Encryption Method:    XTS-AES 128
    Protection Status:    Protection On
    Lock Status:          Unlocked
    Identification Field: Unknown
    Key Protectors:
        Numerical Password
        TPM
```

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.

CHRIS HOFFMAN

Chris Hoffman is Editor-in-Chief of How-To Geek. He's written about technology for over a decade and was a PCWorld columnist for two years. Chris has written for The New York Times, been interviewed as a technology expert on TV stations like Miami's NBC 6, and had his work covered by news outlets like the BBC. Since 2011, Chris has written over 2,000 articles that have been read nearly one billion times---and that's just here at How-To Geek.

READ FULL BIO »

The above article may contain affiliate links, which help support How-To Geek.