How to enable or disable UEFI Secure Boot in BIOS

Have you ever tried installing a second operating system on Windows? If so, you've likely encountered some UEFI Secure Boot errors during the process. So, what is UEFI Secure Boot, and how do you enable or disable it in the BIOS to fix these errors?

If Secure Boot doesn't recognize the code the user is trying to install, it will immediately stop the execution process. Secure Boot is quite useful in preventing malicious code from running on your system. Additionally, this feature also prevents some legitimate operating systems from running, such as Kali Linux, Android x86, or TAILS.

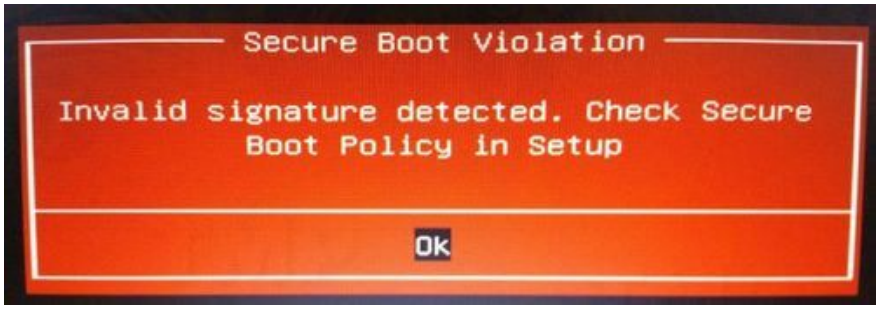
Instructions on how to enable and disable UEFI Secure Boot

This article from TipsMake will guide you **on how to enable or disable UEFI Secure Boot in the BIOS** to allow you to run any dual operating system on your system.

Article contents:
1. UEFI Secure Boot
2. Disable UEFI Secure Boot
3. Enable Secure Boot
4. Troubleshooting
5. Trusted Boot

1. What is UEFI Secure Boot?

Before learning how to enable or disable UEFI Secure Boot in BIOS, you should understand what **UEFI** is and how it differs from BIOS. Refer to the content below for more detailed information. Secure Boot is a feature of **the Unified Extensible Firmware Interface (UEFI)** . UEFI is an alternative interface to BIOS, found on many devices. Essentially, UEFI is a more advanced firmware interface with more customization and technical options.



Secure Boot is something on top of a security gateway. It analyzes code before a user executes it on their system. If the code has a valid digital signature, Secure Boot will allow it through the gateway. If the code has an unrecognized digital signature, Secure Boot will block it, and the system will require a restart.
Sometimes, in certain cases, your code is secure, and the code is obtained from a trusted source, but it may not have a digital signature in the Secure Boot database.
For example, you can download many Linux distributions directly from the developer's website, using checksum software to verify for counterfeit distributions. However, Secure Boot will still reject some operating systems and certain types of code (such as drivers and hardware).

2. How to disable UEFI Secure Boot:
For security reasons, TipsMake recommends against disabling Secure Boot. Secure Boot protects your system from certain variants of malware, such as rootkits and bootkits.
Note that re-enabling UEFI Secure Boot may require a BIOS reset. While a BIOS reset doesn't erase your system data, it will remove custom BIOS settings. In some cases, users may even be permanently unable to re-enable Secure Boot.

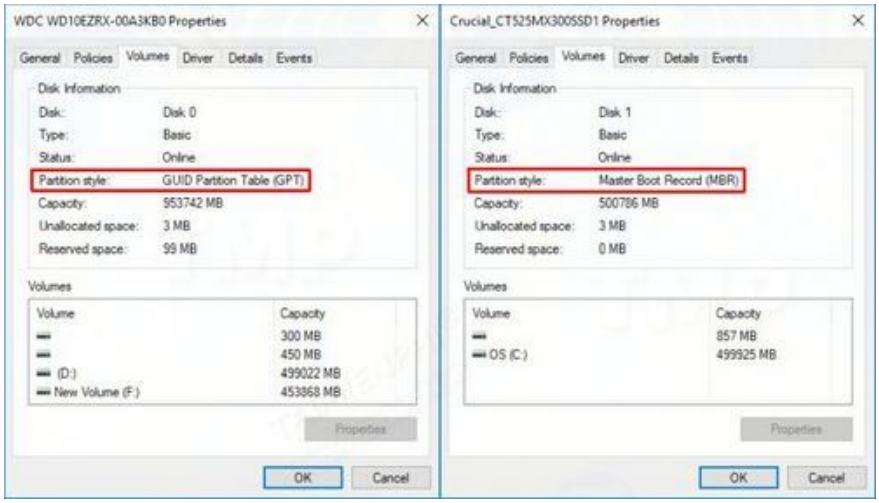
Here's how to disable UEFI Secure Boot:
Step 1: Turn off your computer, then turn it back on. During startup, press a key to access the BIOS. Depending on the hardware and model, the BIOS access key is usually **F1, F2, F12, Esc** , or **Del** .
Windows users can press and hold **the Shift key** and click **Restart** to access the Advanced Boot menu. Then select **Troubleshoot** => **Advanced Options: UEFI Firmware Settings** .
Step 2: Find the **Secure Boot** option and set it to **Disabled.** The Secure Boot option is usually located in the Security tab, Boot tab, or Authentication tab.
Step 3 : Save the changes and exit the window. Your system will then restart.
You have successfully disabled (turned off) Secure Boot.

3. How to Re-enable Secure Boot
If you wish, you can re-enable Secure Boot to protect your system from malware and unauthorized code. If you installed an unsigned operating system directly, you will have to completely erase all traces and uninstall any unsigned software or operating system before re-enableing Secure Boot. Otherwise, the process will fail.
Step 1: Uninstall any unsigned operating system or hardware that you installed when Secure Boot was disabled.
Step 2: Turn off your computer, then turn it back on. During startup, press the key to access the BIOS .
Depending on the type of hardware and computer model, the BIOS access key is usually F1, F2, F12, Esc, or Del.

Windows users can press and hold **the Shift key** and then click **Restart** to access the Advanced Boot menu.
Step 3 : Find the **Secure Boot** optionand set it to **Enabled** . The Secure Boot option is usually located in the Security tab, Boot tab, or Authentication tab.
Step 4: If Secure Boot is not enabled, try resetting the BIOS to its original factory settings. After restoring the settings to their original state, try enabling Secure Boot again.
Step 5 : Save the changes and exit the window. Your system should then restart.
If the system fails to boot, try disabling Secure Boot again.

4. Fixing Secure Boot Failure

There are a few minor patches we can try to boot the system with Secure Boot enabled.
- Ensure UEFI settings are enabled in the BIOS menu, meaning Legacy Boot Mode and related settings are disabled.
- Check the hard drive partition type: UEFI requires GPT partition type, while Legacy BIOS settings require MBR. To check the hard drive partition type, type " **Computer Management"** in the Search box on the Start Menu, then click on the search result. Select **Disk Management** from the menu, then your main drive, right-click on it and select **Properties** . Your partition type is listed here.
If you want to convert from MBR to GPT, the only option to change that partition type is to back up your data and then wipe the hard drive.
- Some firmware managers have a **"Restore Factory Keys"** option , located in the same tab as other Secure Boot options. If this option is available, restore the Secure Boot keys to their original state. Then save and exit the manager, and restart your system.



5. Trusted Boot:

Trusted Boot starts where Secure Boot stopped, but only applies to Windows 10 digital signatures. When UEFI Secure Boot exceeds the threshold, Trusted Boot verifies aspects of Windows, including drivers, boot files, and more.
Similar to Secure Boot, if Trusted Boot detects corrupted or malicious components, it will refuse to load. However, the difference is that Trusted Boot can sometimes automatically repair these issues, depending on the severity.

The article on TipsMake just showed you how to enable or disable UEFI Secure Boot in the BIOS. Disabling Secure Boot can cause several other risks. Currently, Secure Boot is considered more useful than ever, given the increasing prevalence of ransomware, rootkits, and other malicious variants. Secure Boot provides the UEFI

system with a higher level of system authentication, giving users complete peace of mind.