Secure Boot

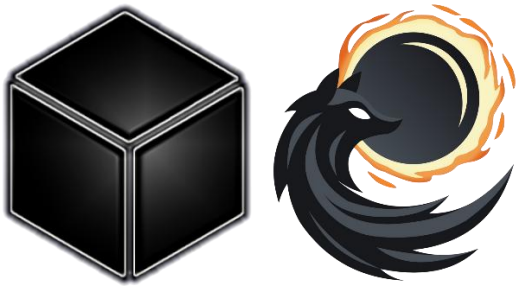
and

TPM Activation Guide

Compatible with Intel and AMD Motherboards

Full compatibility with BlackBox

Black Security – Black Wolf



Technical document prepared by P3ninha Optimizations, specialist in system optimization, audio enhancement, and network optimization for anti-cheat compatibility.

Professional Overview — P3ninha Optimizations

🚀 **Exclusive network optimization technology with proven results.**
🎯 **Full performance focus for top-tier competitive gamers.**
✅ **Approved and authorized by BlackBox Anti-Cheat** and compatible with other security systems.

Secure Boot — What It Is and Why It Matters

🔒 **Protection and legitimacy:** why anti-cheats require Secure Boot.
🏆 **Ensures fair competition** and helps prevent cheating.

Secure Boot — Technical Notes and Disk Conversion

📌 Critical points and recommendations for correct activation.
⚙️ Technical adjustments for **maximum performance** without compromising security.
💡 **P3ninha handles this for you** — including audio tuning and network optimization for superior results.
✅ Final step: **activation verification**.

Step-by-Step by Motherboard Brand

1️⃣ **ASUS**
2️⃣ **MSI**
3️⃣ **Gigabyte**
4️⃣ **ASRock**
5️⃣ **Colorful** *(generic)*
6️⃣ **Mancer** *(generic)*
7️⃣ **Pichau** *(generic)*

About P3ninha Optimizations

🎮 Who I Am

I am a specialist in system optimization for competitive gamers, focusing on compatibility with anti-cheat solutions such as **BlackBox** and **Black Security**. My goal is to deliver maximum performance without compromising stability or security.

🚀 What I Do

- Full system optimization to reduce delay and input lag.
- **Audio enhancement** for clearer, more precise, and long-range sound detection.
- **Exclusive network optimization technology** for faster server responses and greater shot accuracy.

🏆 Why Choose P3ninha

- Proven results tested by professional eSports players.
- Full compatibility with the most popular anti-cheat systems.
- Specialized support for both **Intel** and **AMD**, on desktops and laptops.

📍 Mission

To ensure that competitive players have access to the same cutting-edge technology used by professional teams, so they are always one step ahead of their opponents.

Contact:

+55(19) 994473560

Link WhatsApp

Link Instagram @p3ninha

About BlackBox Anti-Cheat and Black Security

BlackBox Anti-Cheat

BlackBox is an advanced cheat detection system that operates at the kernel level — the same privilege layer as the operating system. This ensures that monitoring and system integrity checks occur before Windows and the game are fully loaded, making it extremely difficult for cheats or unauthorized modifications to go undetected.

Its approach follows the "black box" concept: the internal detection logic is protected from reverse engineering, preventing cheaters from discovering ways to bypass it.
The use of Secure Boot and TPM 2.0 is part of its security requirements, ensuring that the PC boots in a clean state, free from malicious changes, and maintains the legitimacy of online competitions.

Black Security

Black Security is another anti-cheat system designed for high-level competitive gaming, also focusing on hardware security and system integrity. Like BlackBox, it uses advanced techniques to prevent tampering, and it can work alongside Secure Boot and TPM to provide a safe, reliable environment for competitive matches.

Key Technical Points

- **Kernel-level operation: provides complete control over processes and drivers, blocking even advanced cheats.**
- **Hardware-level protection: requires Secure Boot and TPM 2.0, creating a barrier against system alterations before boot.**
- **Official competition compatibility: used by platforms seeking to ensure fair play and prevent result manipulation.**

Contact Link do Discord

Secure Boot — Why It’s Essential for Anti-Cheat Systems

Secure Boot is a security feature built into modern motherboards that ensures the system only boots using trusted, signed software.
For anti-cheat solutions like BlackBox or Black Security, it plays a vital role in preventing the use of modified or unauthorized system components that could enable cheating.

Why Anti-Cheats Require It

- **Integrity & Fair Play: Ensures the game runs on a verified, tamper-free environment.**
- **Prevention of Rootkits & Boot-Level Hacks: Blocks low-level malicious tools before Windows even starts.**
- **Compliance: Some competitive platforms will not allow you to connect without it enabled.**

Important Warnings Before Activation

Enabling Secure Boot isn’t just flipping a switch — there are technical details you must understand:

- **CSM Must Be Disabled: Secure Boot only works in pure UEFI mode. Disabling CSM (Compatibility Support Module) can cause your PC not to display video output if your Windows installation uses the MBR partition style instead of GPT.**
- **Possible Need for Disk Conversion: If your system is still on MBR, it may require conversion to GPT before enabling Secure Boot — otherwise, the PC may fail to boot.**
- **Not All Boards Have TPM 2.0: While many newer Intel and AMD motherboards include TPM 2.0 or firmware equivalents (PTT for Intel, fTPM for AMD), some older or budget boards may not support it at all.**

💡 **Professional Tip: If you’re unsure about any of these steps, let P3ninha Optimizations handle the process. We ensure full compatibility while also applying exclusive system, audio, and network optimizations for the best competitive performance.**

🔧 *Starting the Procedures — Enabling Secure Boot and TPM*

Below, you will find a step-by-step guide to enable Secure Boot and TPM 2.0 on the most common motherboard brands, for both AMD and Intel systems.

⚠ Important Notice

During the process, you will need to disable CSM to enable UEFI mode. If your drive is formatted as MBR, your system may fail to display video output after reboot.
Some motherboard models — especially older ones — do not have TPM 2.0, either as a physical chip or integrated in the CPU.

🔍 Initial Recommendations

- **Back up your data before making any changes.**
- **Know how to access the BIOS again (DEL or F2 during startup).**
- **After completing all configurations, press F10 in any BIOS to save and reboot.**

🛠 Process Overview

1. **Disable CSM (enable UEFI mode).**
2. **Enable Secure Boot.**
3. **Enable TPM 2.0 (Intel: PTT | AMD: fTPM).**
4. **Press F10 to save and reboot.**
5. **Verify that everything is enabled correctly.**

✅ How to Check if Secure Boot is Active in Windows

1. **Press Win + R, type msinfo32, and press Enter.**
2. **In the System Information window, look for the field Secure Boot State.**
    - **On = Secure Boot is enabled.**
    - **Off = Secure Boot is disabled.**

🔒 ASUS Guide — Enable Secure Boot and TPM

This guide was created to help users, even those without BIOS experience, to enable Secure Boot and TPM on ASUS motherboards. The procedure is described patiently, step-by-step, with clear instructions.

Enable Secure Boot — Step-by-step

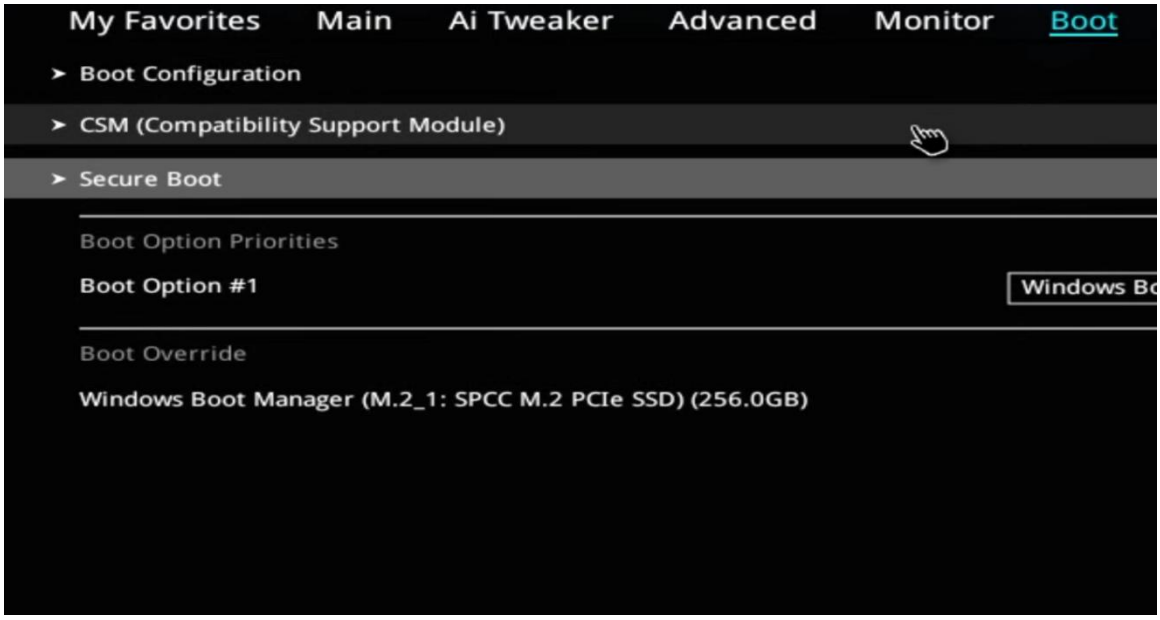
1️⃣ Turn on or restart the computer.

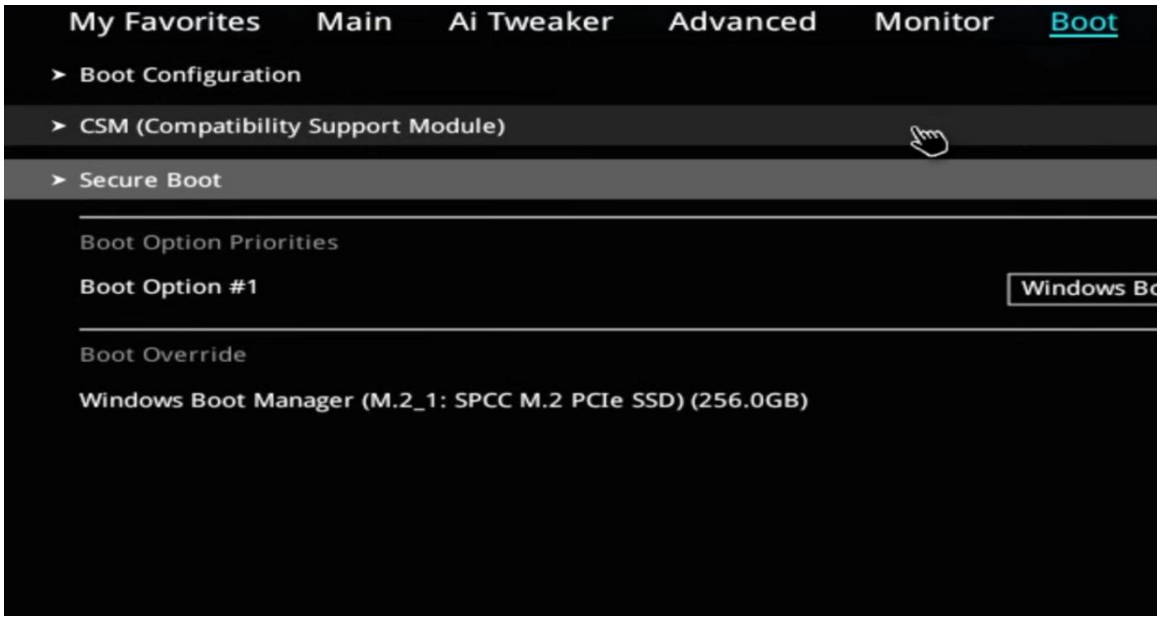
→ When the first screen (ASUS logo) appears, repeatedly press DEL or F2 to enter BIOS.

→ If using a 60% keyboard, press FN + DEL or FN + F2.

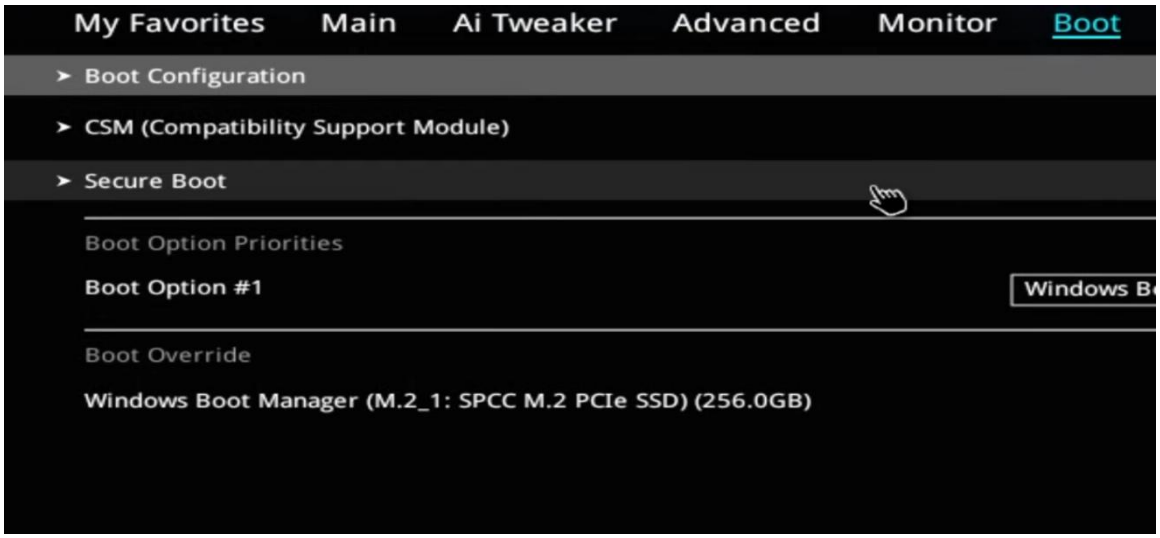
→ Press F7 to enter Advanced Mode.

→ Go to Boot → CSM and change Launch CSM to Disabled. Save and restart.

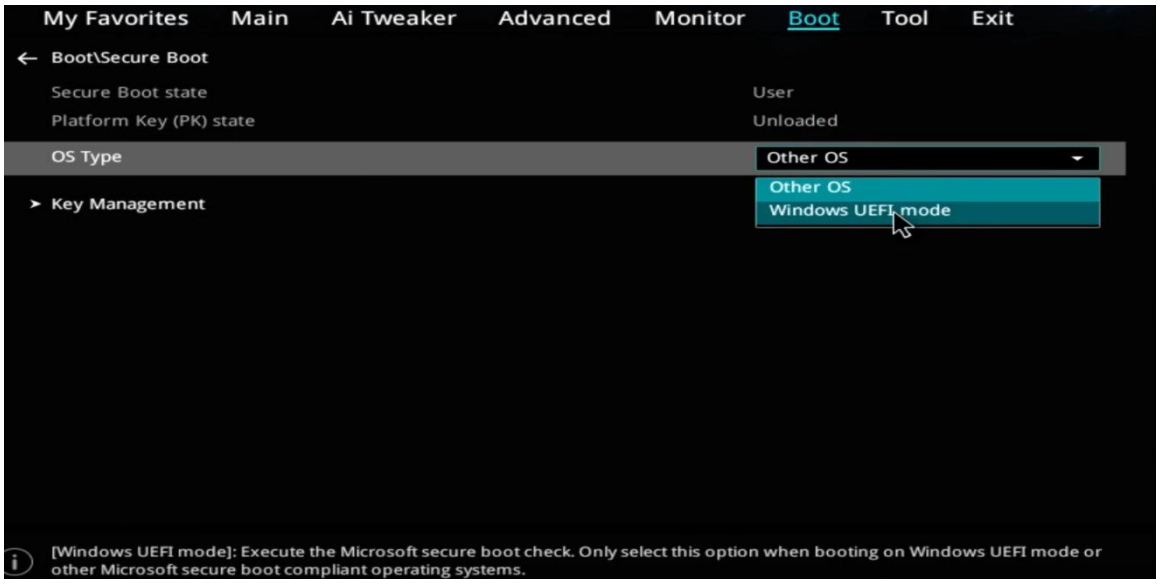




→ Go to Boot → Secure Boot or Advanced → Secure Boot.



→ Inside Secure Boot, locate OS Type, Secure Boot Mode, and Key Management.

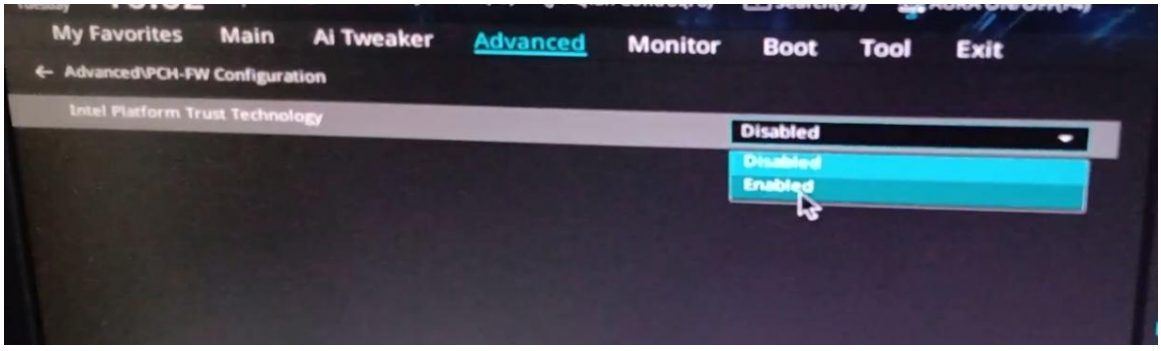


4️⃣ First attempt (Standard): Go to Secure Boot and change it to Enabled. Go to Secure Boot Mode and change it to Standard. If available, change OS Type to Windows UEFI Mode. In Key Management, select Install Default Secure Boot Keys. Save and restart.

5️⃣ If it doesn't work: Return to Secure Boot. Change Secure Boot Mode to Custom. In Key Management, select Install Default Secure Boot Keys or Restore Factory Keys. Save and restart.

Enable TPM (Intel PTT)

→ Go to Advanced → PCH-FW Configuration → Intel Platform Trust Technology → And change it to Enabled.



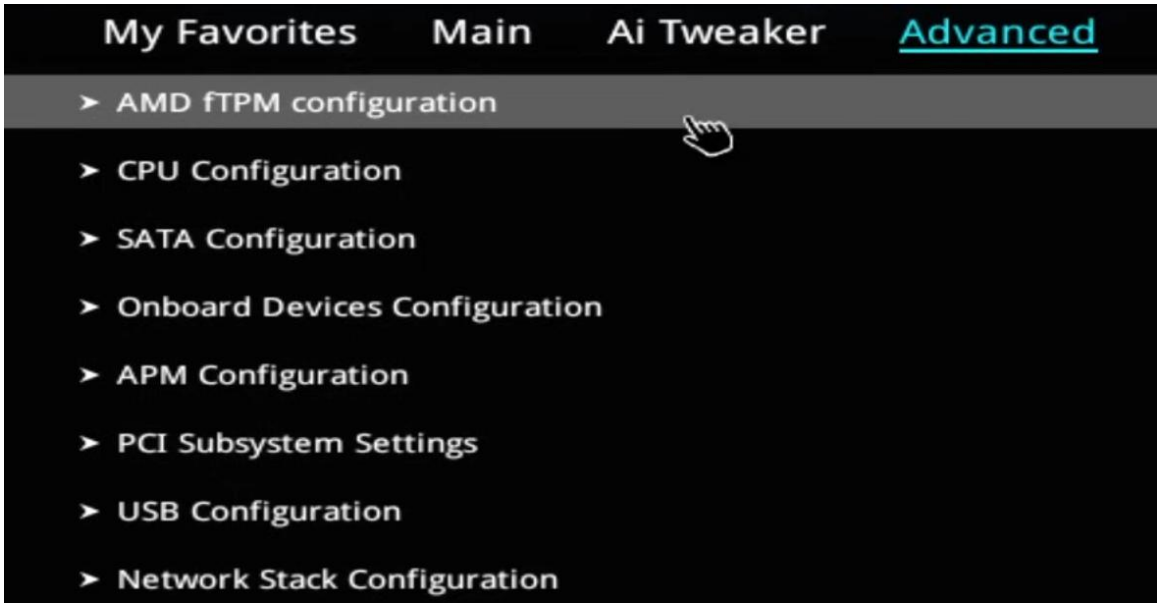
→ If Trusted Computing exists, go to Security Device Support and change it to Enabled.

→ Confirm that the version is TPM 2.0, if available.

→ Save and restart (F10).

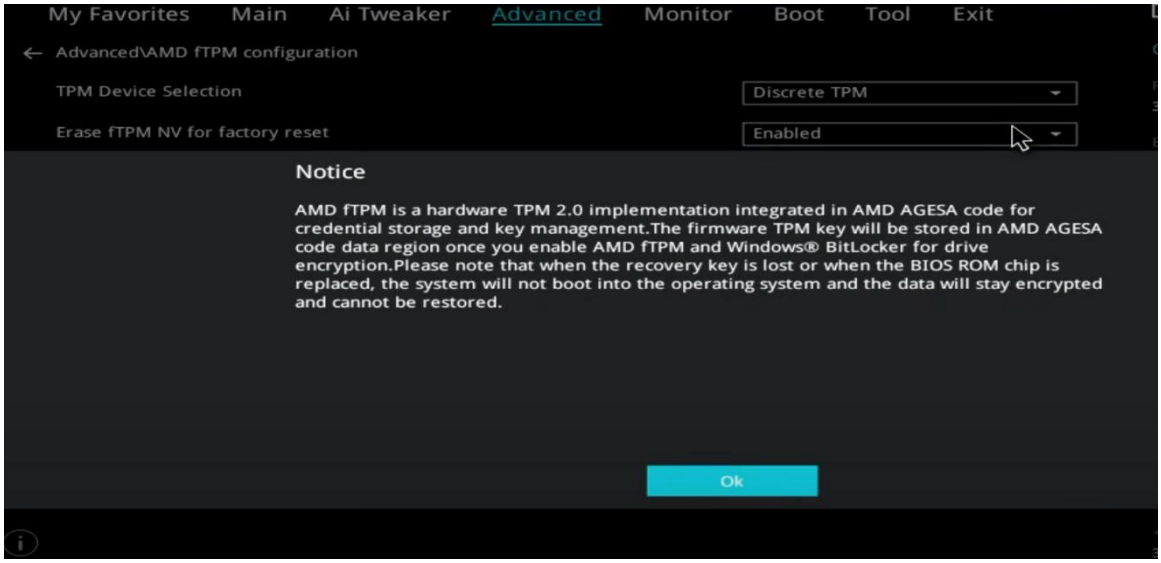
Enable TPM (AMD fTPM)

→ Go to Advanced → AMD fTPM Configuration → TPM Device Selection and change it to Firmware TPM.



→ If not found, check Advanced → Trusted Computing and enable Security Device Support.

→ Confirm that the version is TPM 2.0, if available.



→ Save and restart (F10).

🔒 MSI Motherboards - Secure Boot & TPM Activation Guide

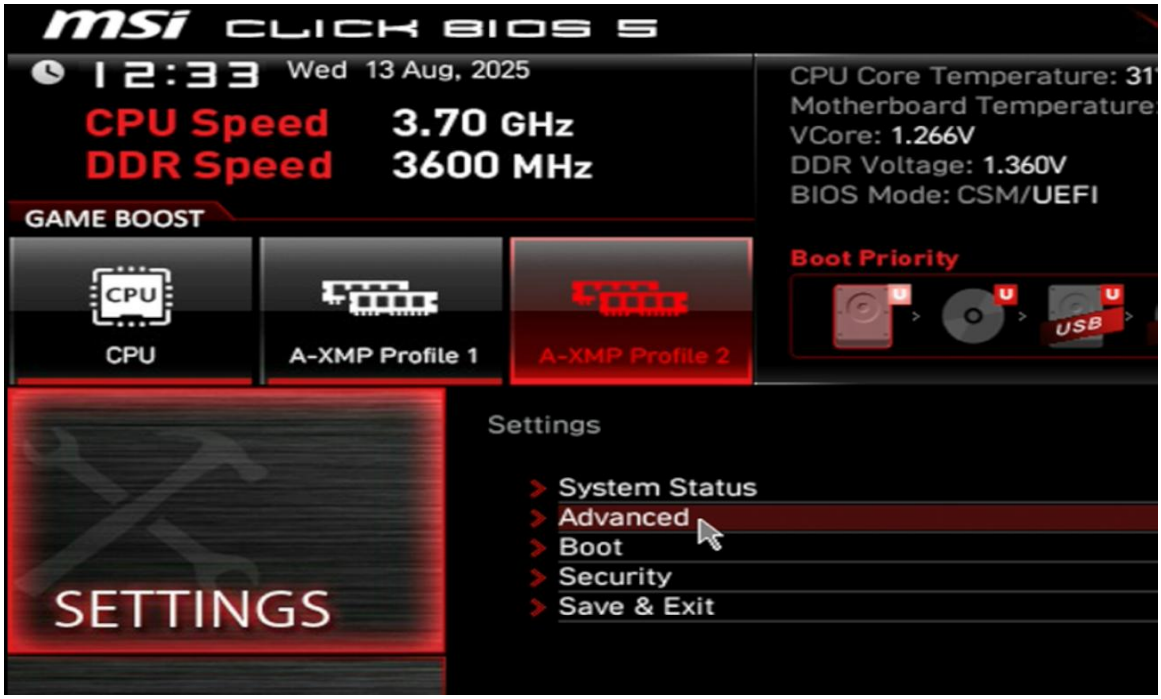
This guide is designed for beginners who have never accessed the BIOS before. We will go step-by-step to disable CSM, activate Secure Boot (Standard and Custom modes), and enable TPM for both AMD and Intel processors on MSI motherboards.

1️⃣ Enter BIOS

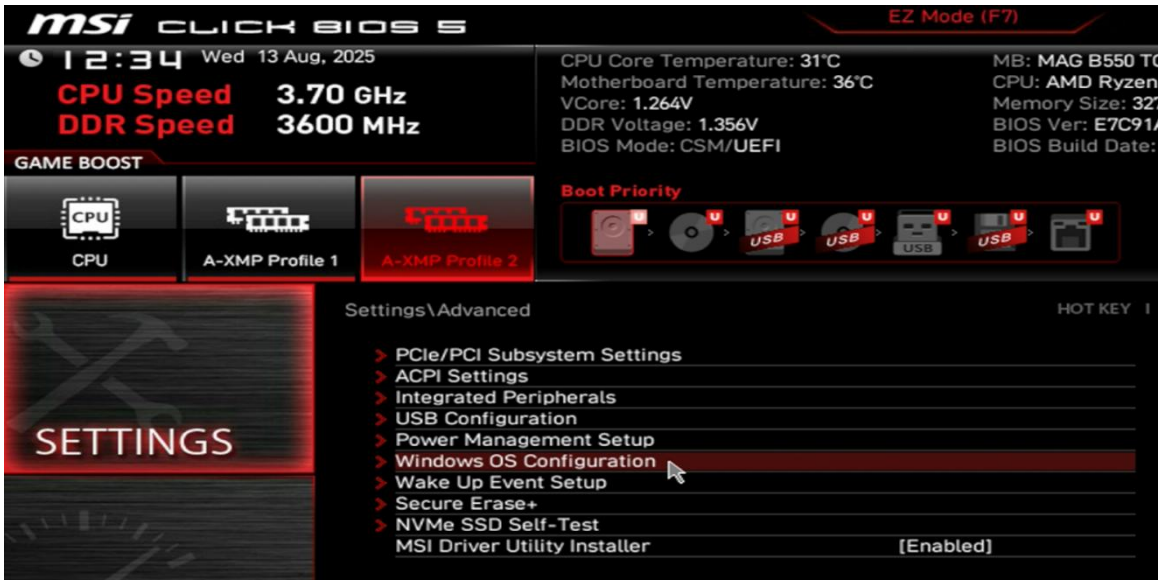
Restart your computer and press the 'Delete' key repeatedly right after powering it on. If using a 60% keyboard, ensure you use the 'Fn' function to access the Delete key. Some MSI motherboards also accept the 'F2' key to enter BIOS. Once inside BIOS, press 'F7' to switch to Advanced Mode.

2️⃣ Disable CSM (Enter UEFI Mode)

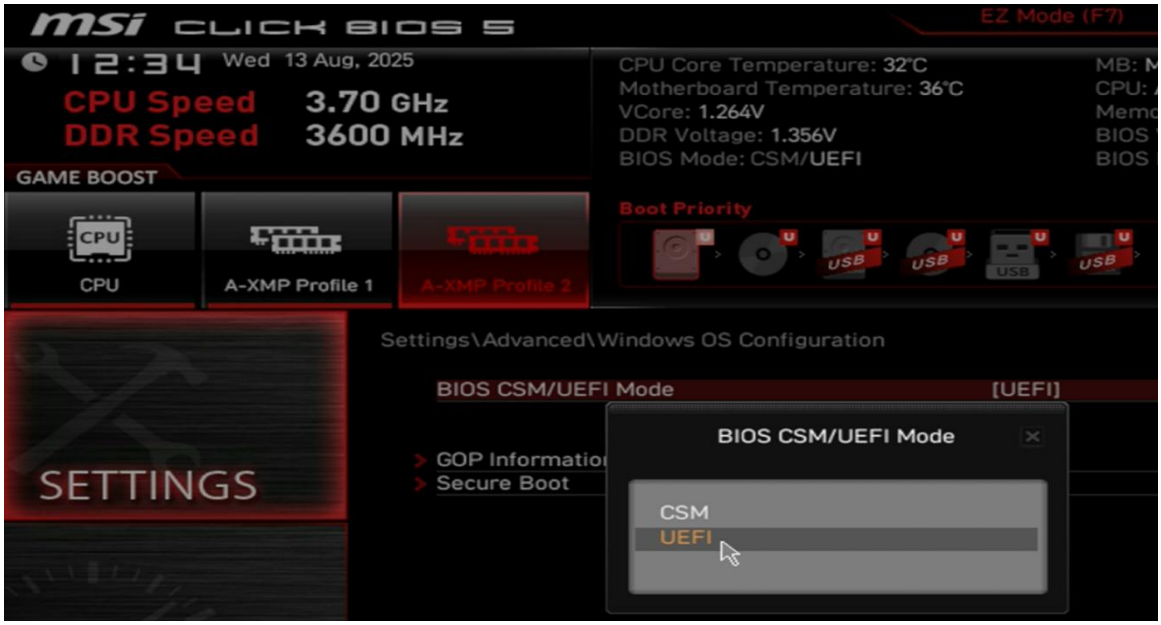
In the BIOS main menu, navigate to: Settings → Advanced



→ Windows OS Configuration

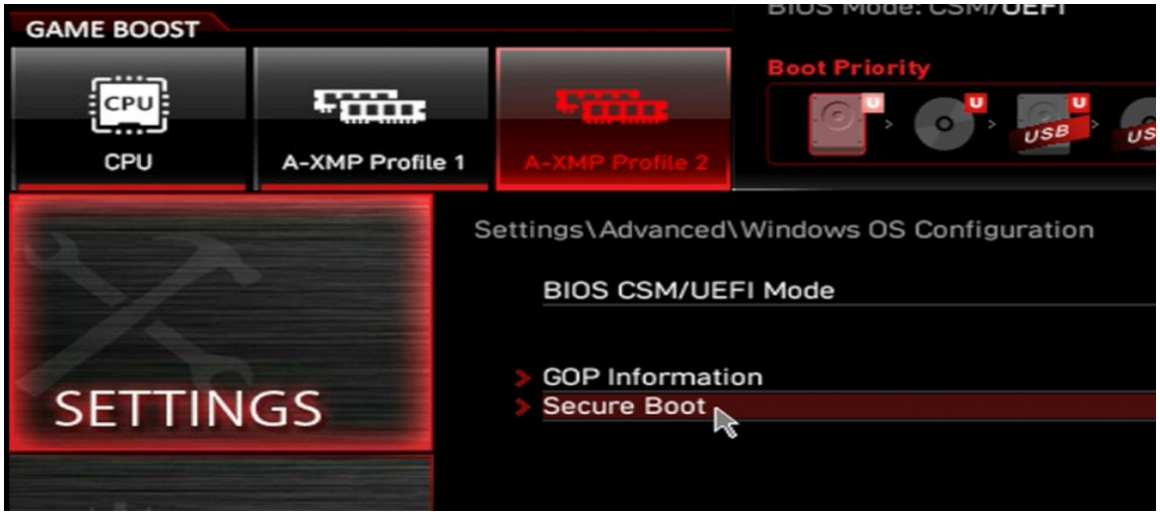


→ BIOS CSM/UEFI Mode → Set to 'UEFI'. On some models, you might see 'Windows 10/11 WHQL Support' instead — set it to 'Enabled'. This step is essential for enabling Secure Boot.

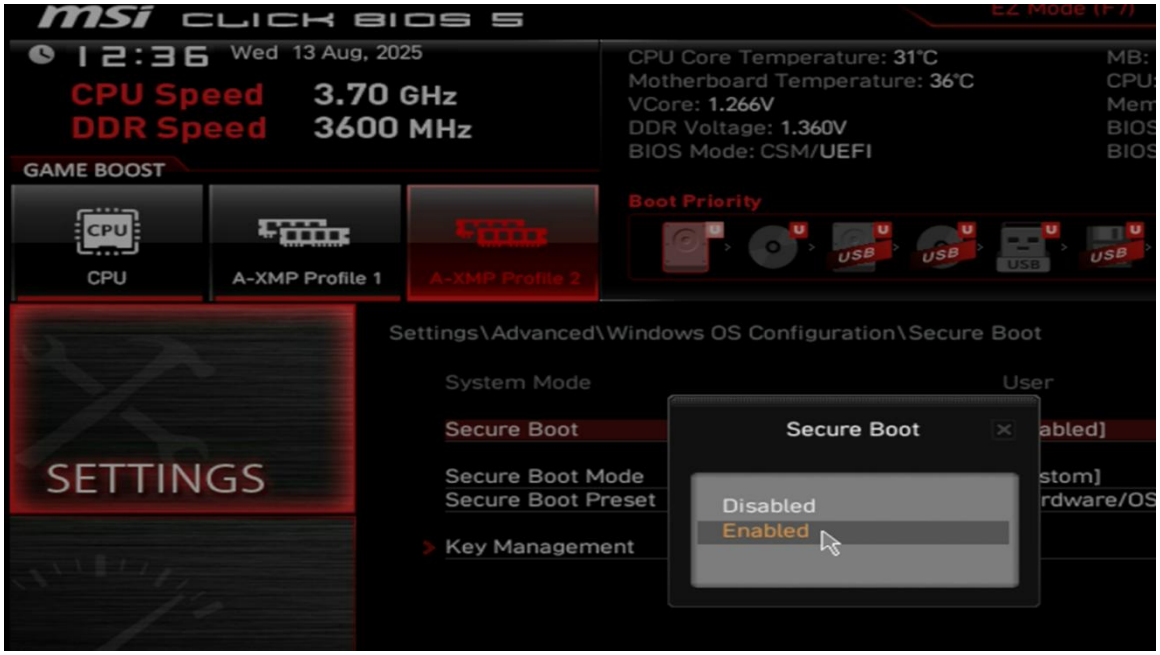


3 Enable Secure Boot — First Attempt (Custom)

Go to: Settings → Advanced → Secure Boot

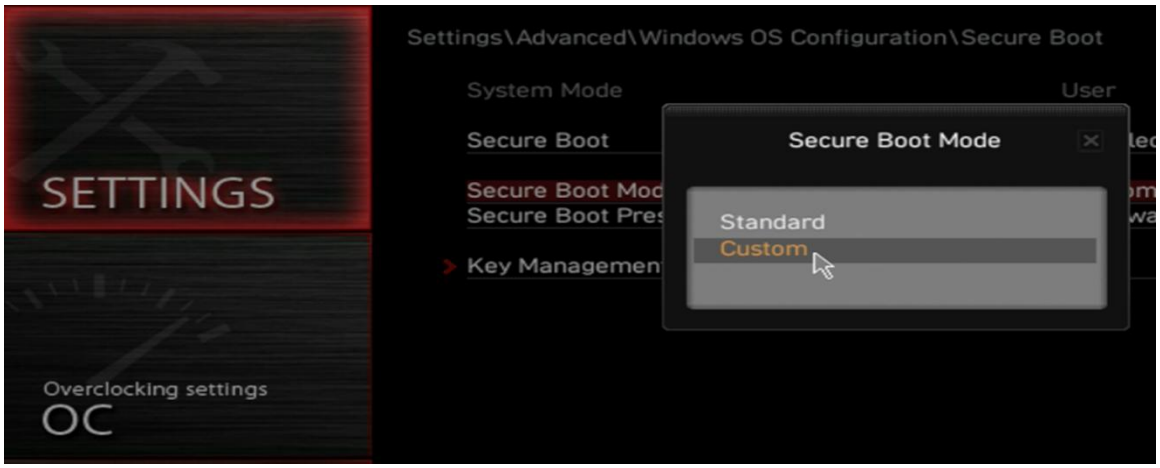


→ Secure Boot → Set to 'Enabled'. Then,

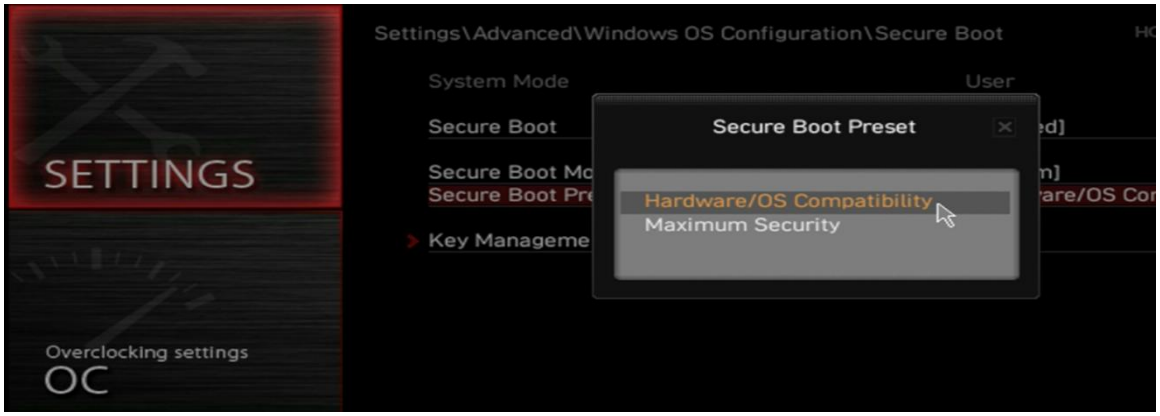


→Secure Boot Mode

→Set to 'Custom'



→ Select Secure Boot Present → Hardware/OS Company.

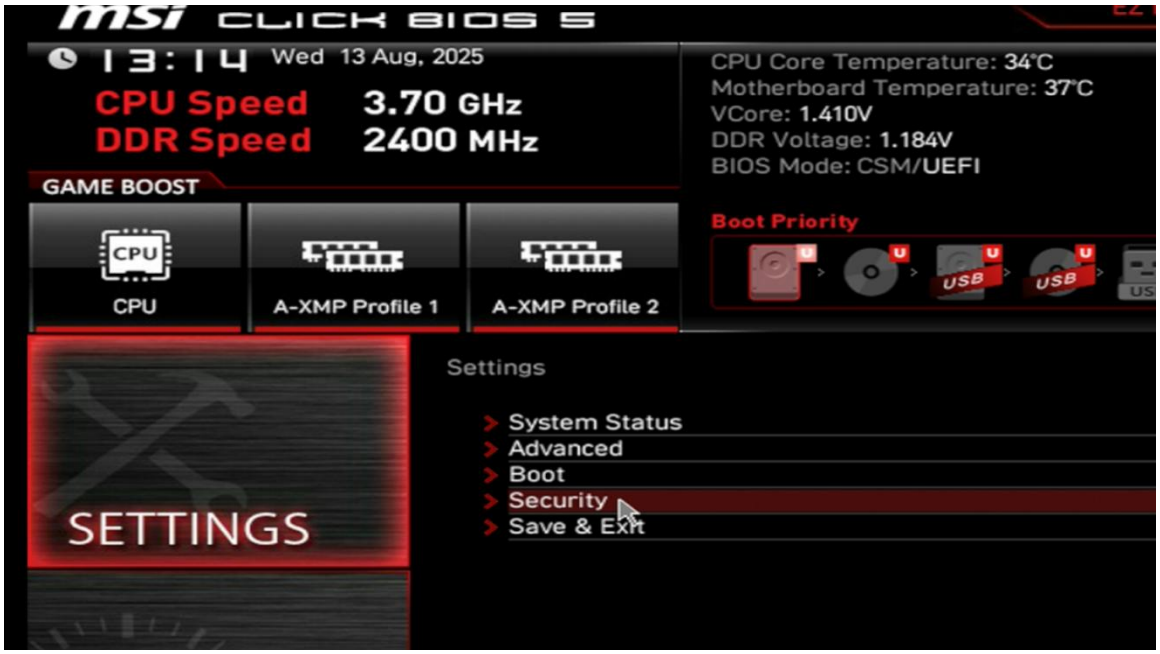


4️⃣ If it doesn’t work — Try Custom Mode

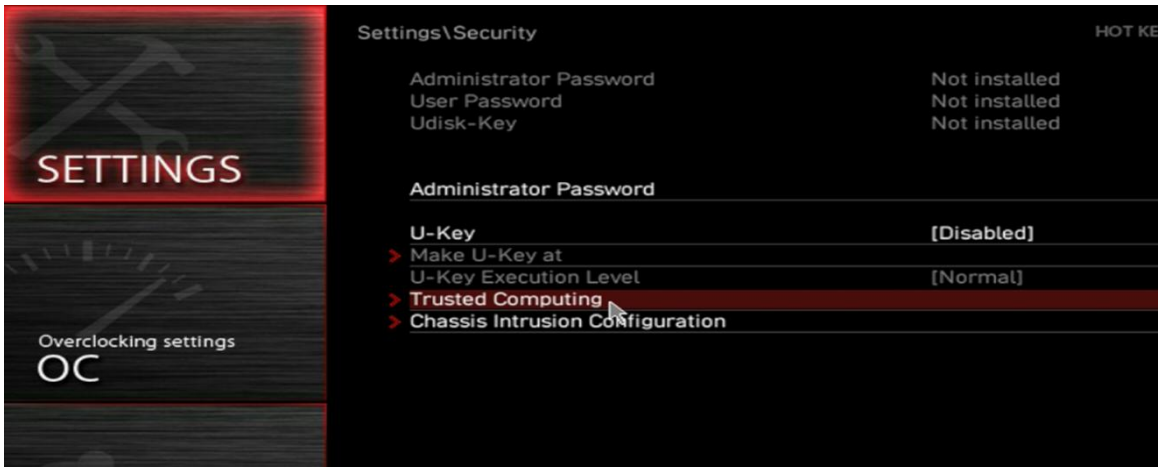
Change Secure Boot Mode to 'Custom', then select 'Install Default Keys'. If Secure Boot Present → Hardware/OS Company is available, keep it active. If it still doesn’t work, try selecting 'Maximum Security' if the option exists.

5 Enable TPM — AMD (fTPM)

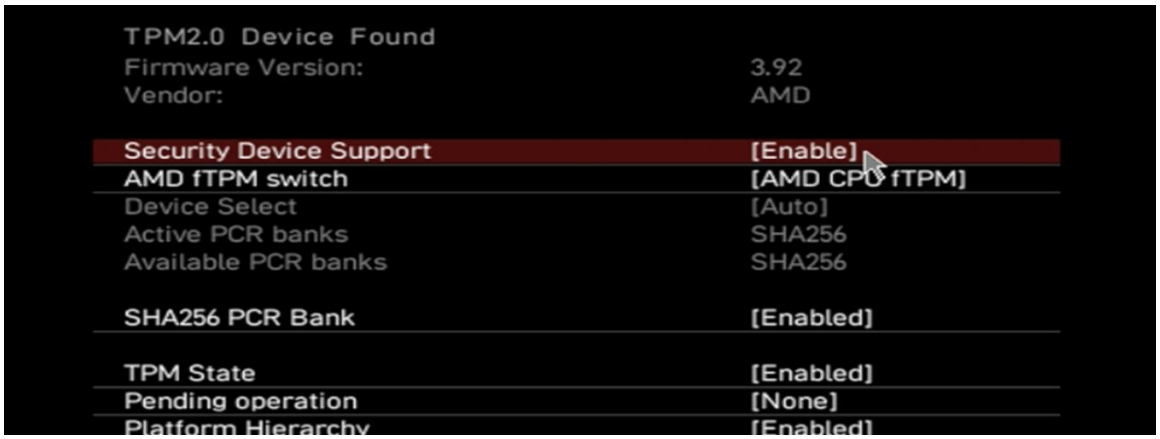
Go to: Settings → Security



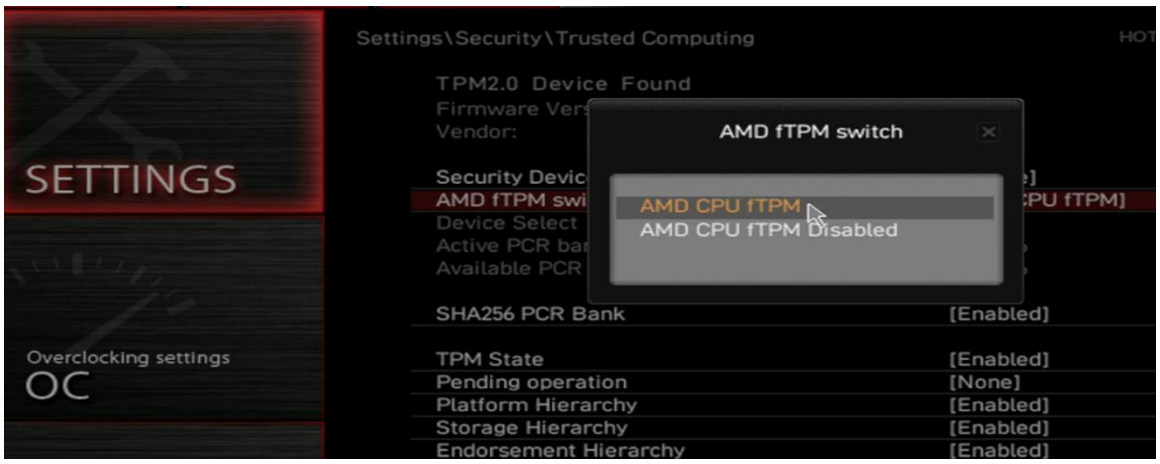
→ Trusted Computing



→ Security Device Support → Set to 'Enabled'.



Then, AMD fTPM Switch → Select 'AMD CPU fTPM'. If the option is missing, check if your BIOS is updated to the latest version.



6 Enable TPM — Intel (PTT)

Go to: Settings → Security → Trusted Computing → Security Device Support → Set to 'Enabled'. Then, Intel Platform Trust Technology (PTT) → Set to 'Enabled'.

7 Final Tips & Verification

Save changes and restart your PC. Once in Windows, press Win + R, type 'tpm.msc' and press Enter — check if TPM is listed as ready. You can also verify Secure Boot by opening 'System Information' (msinfo32) and checking its status.

Detailed Guide – How to Enable Secure Boot and TPM (Gigabyte / AORUS)

This guide is designed for people who have never accessed the BIOS before. We will go step-by-step, in simple language, so you can follow along without fear of breaking anything. First, we try enabling Secure Boot in Standard mode, which is the fastest and easiest way. If that does not work, we will try Custom mode with a key reset. Finally, we will also learn how to enable TPM, which is essential for maximum compatibility with professional anti-cheat systems.

🔐 Enabling Secure Boot

1️⃣ – Entering the BIOS

The BIOS is a settings screen you can access before Windows starts. To enter it:

• Turn on or restart your PC.

• As soon as you see the first screen (motherboard logo), repeatedly press DEL (Delete) or F2.

• 💡 Tip for 60% keyboards: Some smaller keyboards require holding FN while pressing DEL or F2 (example: FN + DEL).

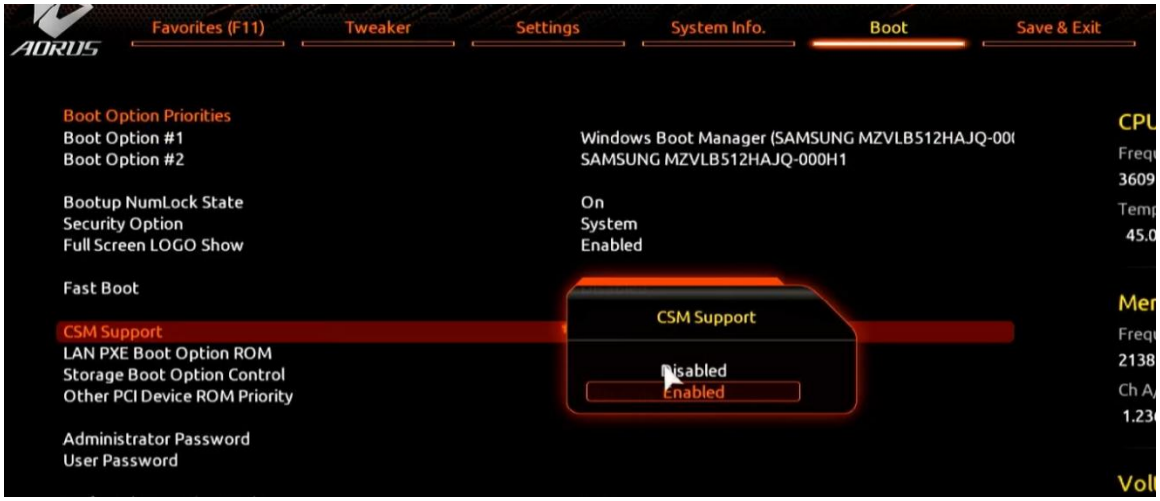
2️⃣ Enable UEFI Mode (Required for Secure Boot)

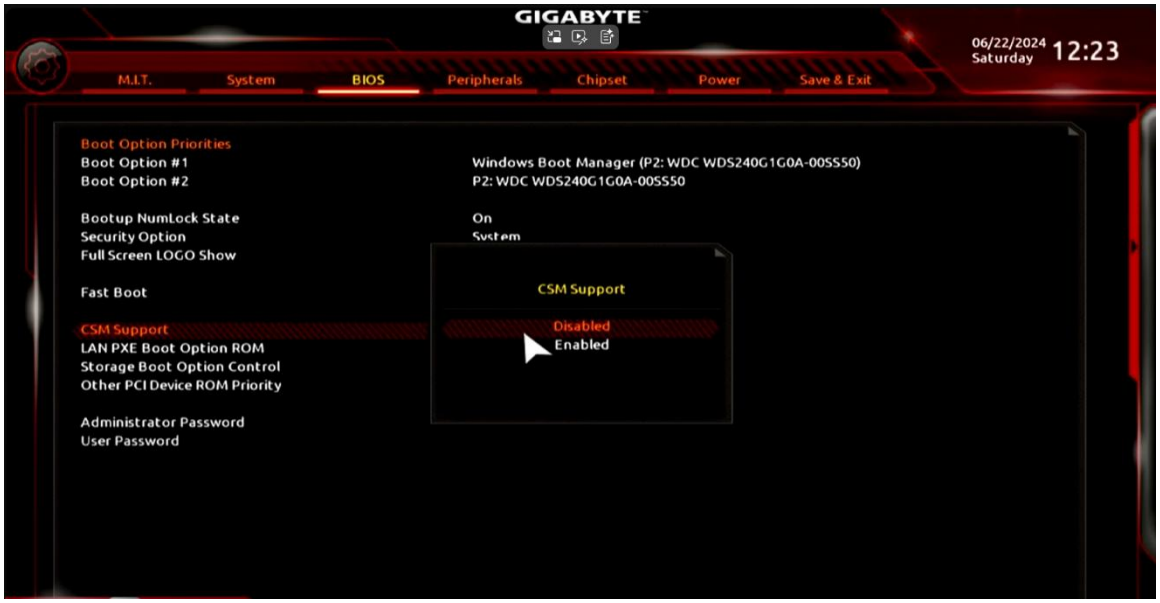
• Once inside the BIOS, press F2 to enter Advanced Mode (or click the button on the screen).

• Find the option called CSM Support (sometimes written as 'Compatibility Support Module').

• It is usually in the BIOS, Boot, or Settings menu.

• Set CSM Support to Disabled.





• Save and restart by pressing F10 (Save & Exit).

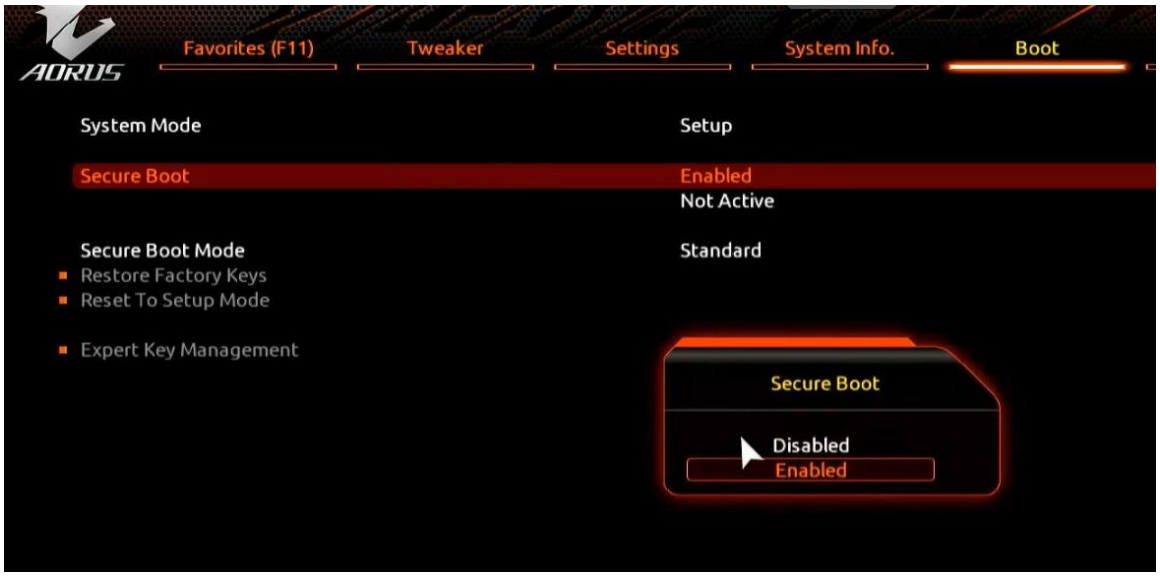
• Your computer will restart and go back to the BIOS automatically.

3️⃣ Finding the Secure Boot Menu

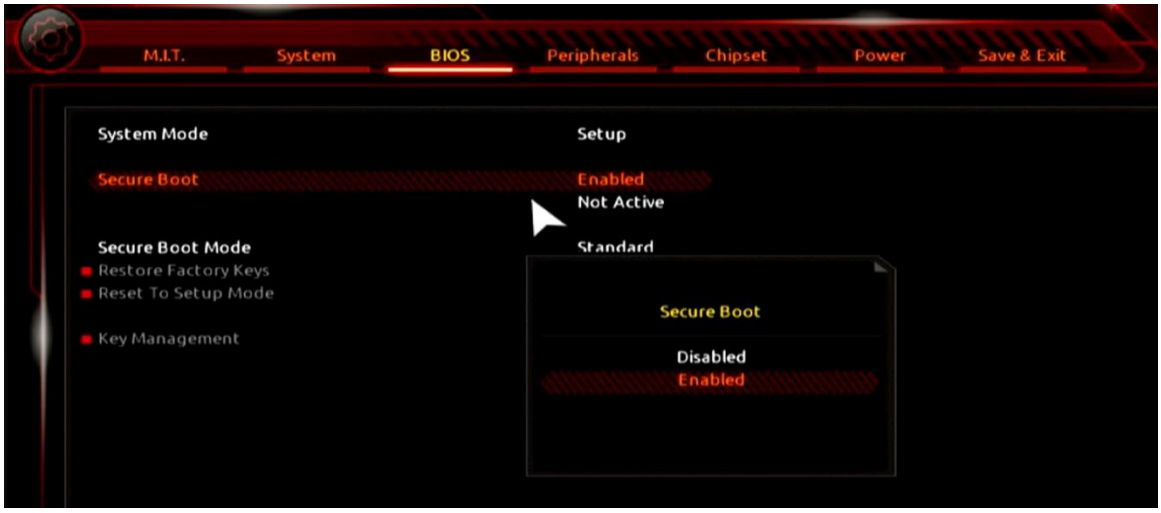
Depending on your BIOS version, the Secure Boot option may be located in different menus. Here are the most common paths:

• Settings → Miscellaneous → Secure Boot (Configurações → Diversos → Inicialização Segura)

• Boot → Secure Boot (Inicialização → Inicialização Segura)



• BIOS → Secure Boot

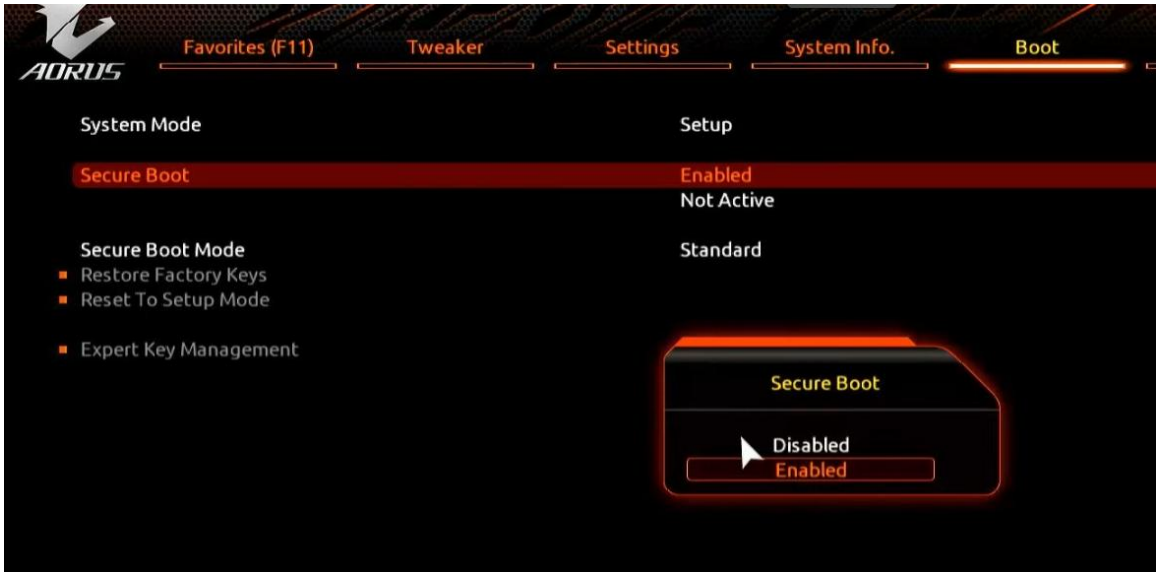


• BIOS Features → Secure Boot (Recursos da BIOS → Inicialização Segura)

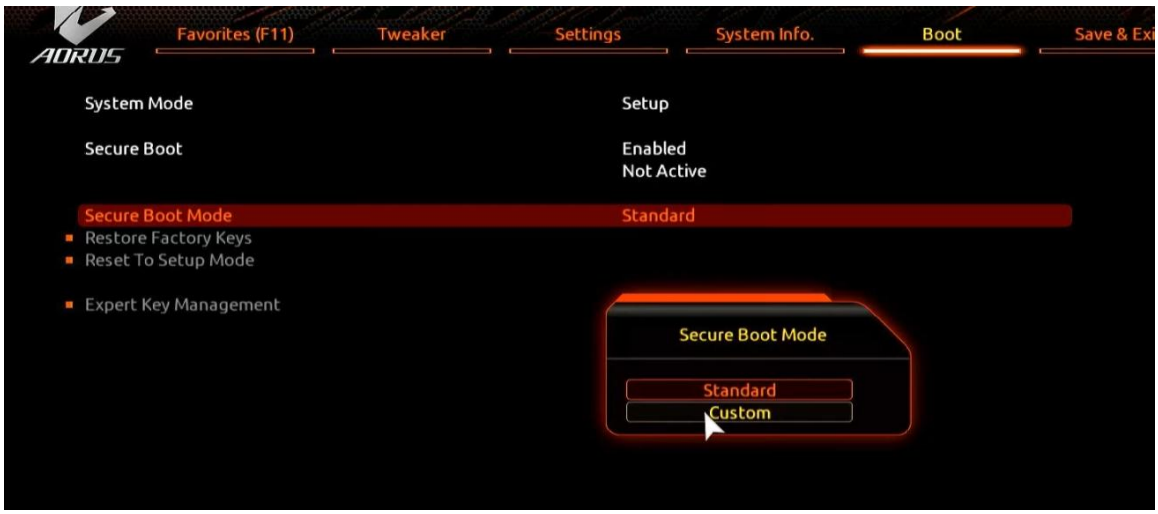
• Settings → Authentication → Secure Boot (Configurações → Autenticação → Inicialização Segura)

4️⃣ First Attempt: Standard Mode

• Set Secure Boot to Enabled.



• In Secure Boot Mode, choose Standard.



• Save changes (F10) and restart.

5️⃣ If Standard Mode Does Not Work

• Go back to the Secure Boot menu.

• Change Secure Boot Mode to Custom.

• Select Install Factory Default Keys or Reset to Setup Mode → Install Default Keys.

• Save (F10) and restart.

6️⃣ If It Still Does Not Work

• Use the option Load Optimized Defaults (sometimes called 'Load Setup Defaults').

• Repeat the process from Step 2 (Enable UEFI Mode).

📌 Quick Summary for Gigabyte/AORUS

Step	BIOS Path (English / Portuguese)	Action
1	BIOS / Boot / Settings (BIOS / Inicialização / Configurações) → CSM Support (Suporte CSM)	Disabled / Desativado
2	Secure Boot (Inicialização Segura)	Enabled / Ativado
3	Secure Boot Mode (Modo de Inicialização Segura)	Standard / Padrão (or Custom / Personalizado)
4	Custom Mode (Personalizado)	Install Default Keys / Instalar Chaves Padrão

🛡️ Enabling TPM

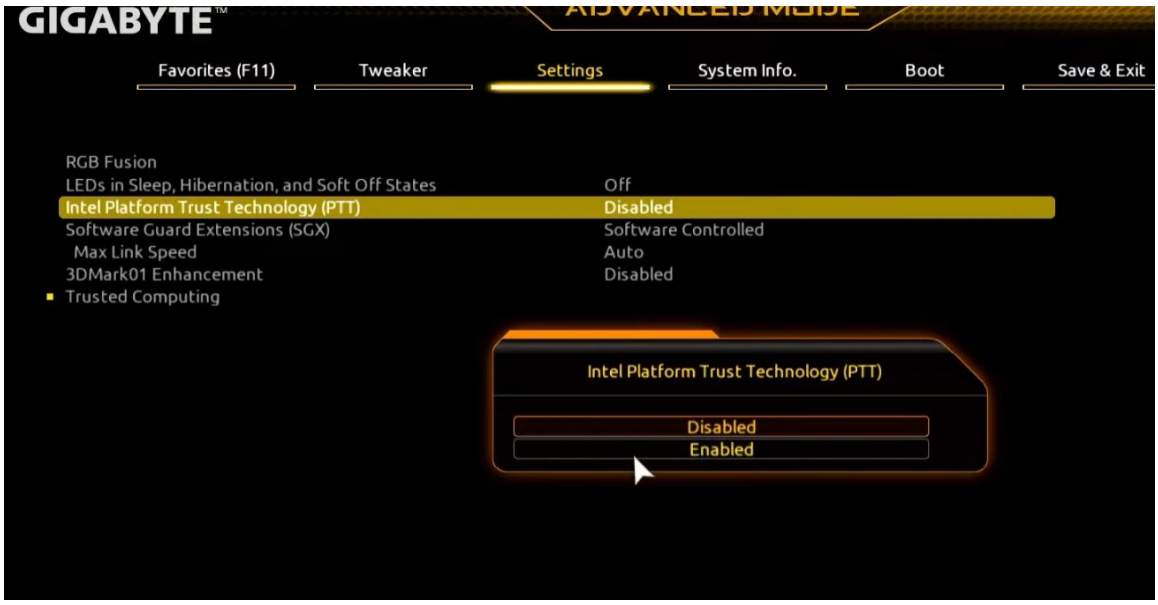
1️⃣ For Intel Processors

• Enter the BIOS again (DEL or F2, or FN + DEL or FN +F2 for 60% keyboards).

• Go to Advanced Mode (F2).

• Main path: Settings → Miscellaneous → Trusted Computing.

• Alternative path: Peripherals → Intel Platform Trust Technology (PTT).



• Set Security Device Support to Enabled.

• Confirm that Intel PTT is Enabled and TPM version is 2.0.

• Save (F10) and restart.

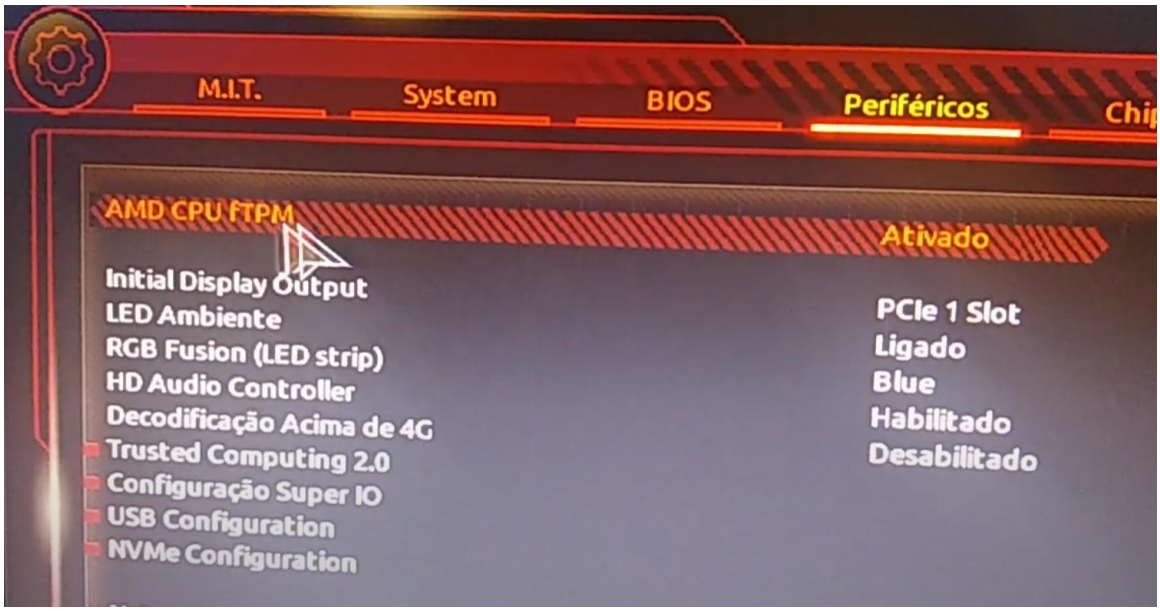
2️⃣ For AMD Processors

• Enter the BIOS again (DEL or F2, or FN + DEL or FN +F2 for 60% keyboards).

• Go to Advanced Mode (F2).

• Main path: Settings → Miscellaneous → Trusted Computing.

• Alternative path: Peripherals → AMD CPU fTPM.



• Set Security Device Support to Enabled.

• Confirm that AMD fTPM is Enabled and TPM version is 2.0.

• Save (F10) and restart.

🔒 ASRock Guide - Enable Secure Boot and TPM

Procedure designed for people who have never accessed the BIOS before. We will enable Secure Boot and TPM (fTPM for AMD and PTT for Intel) on ASRock motherboards in a simple, step-by-step way.

1️⃣ Enter the BIOS

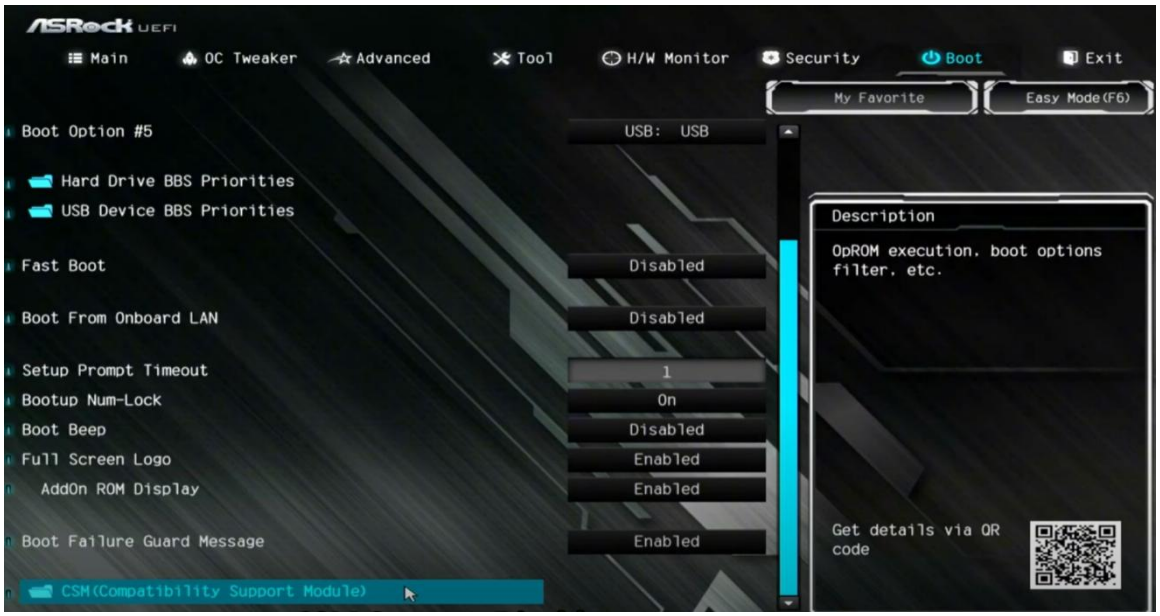
→ Turn on or restart the PC.

→ As soon as the first screen appears (logo/POST), repeatedly press DEL (Delete) or F2 until you enter the BIOS.

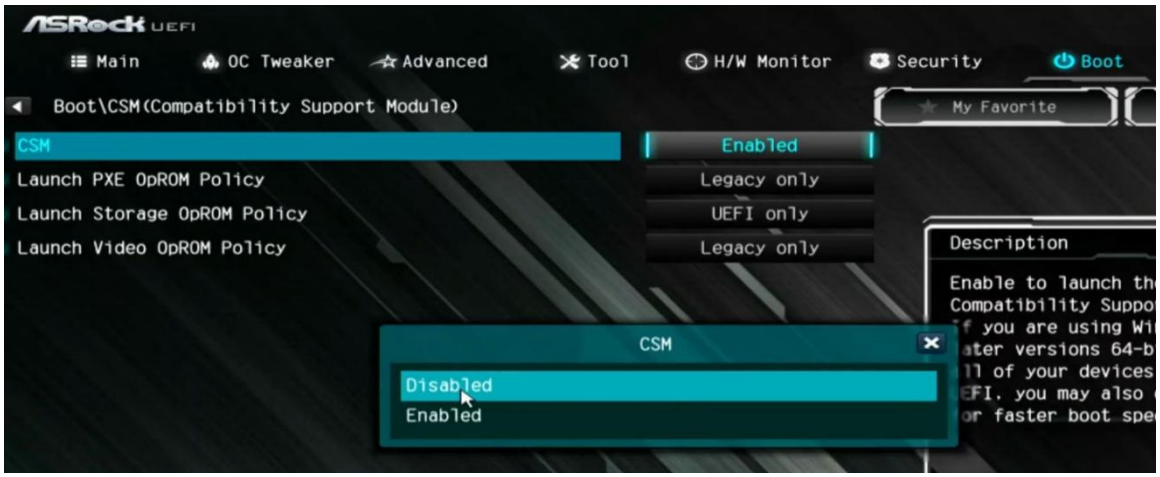
→ If your keyboard is 60%, hold the FN key and press DEL or F2 (e.g., FN + DEL).

2️⃣ Disable CSM (Switch to UEFI mode)

→ Go to Boot → CSM (Compatibility Support Module).



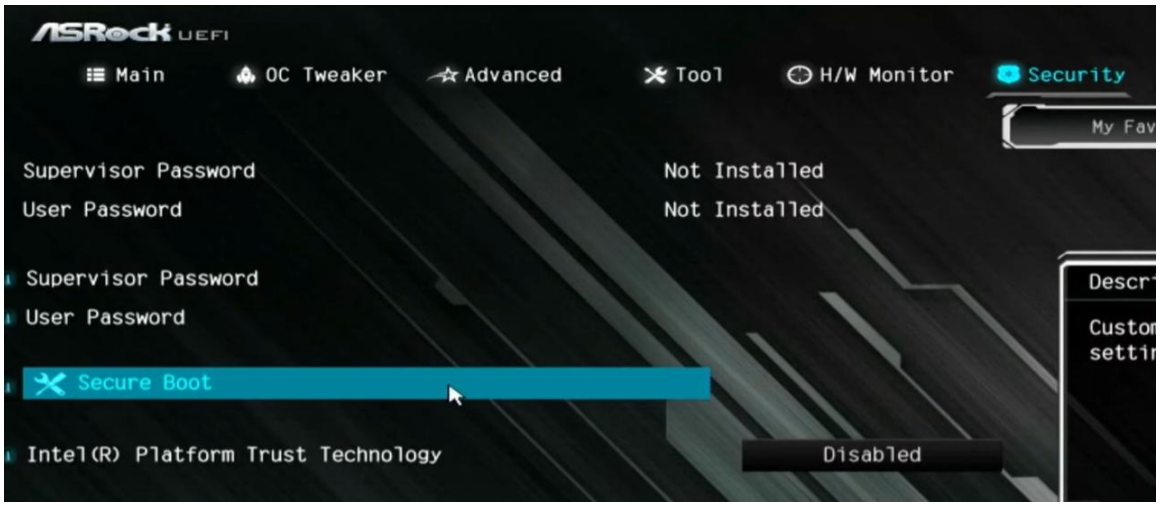
→ Go to Launch CSM and change to Disabled.



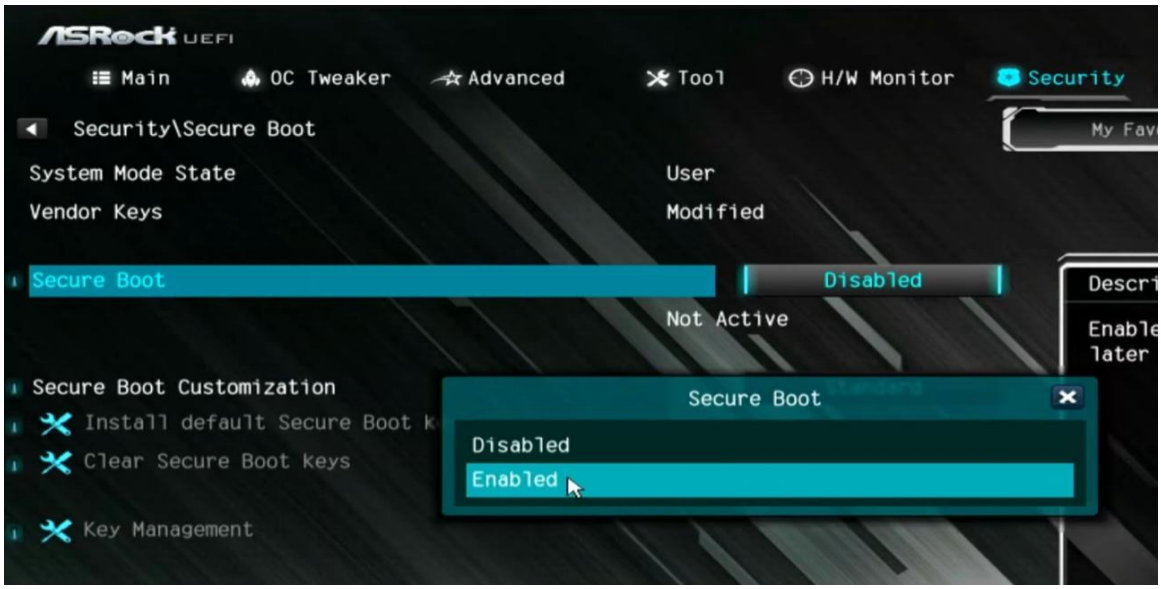
→ Press F10 to save and restart; the PC will usually return to the BIOS.

3 Enable Secure Boot — first attempt (Standard)

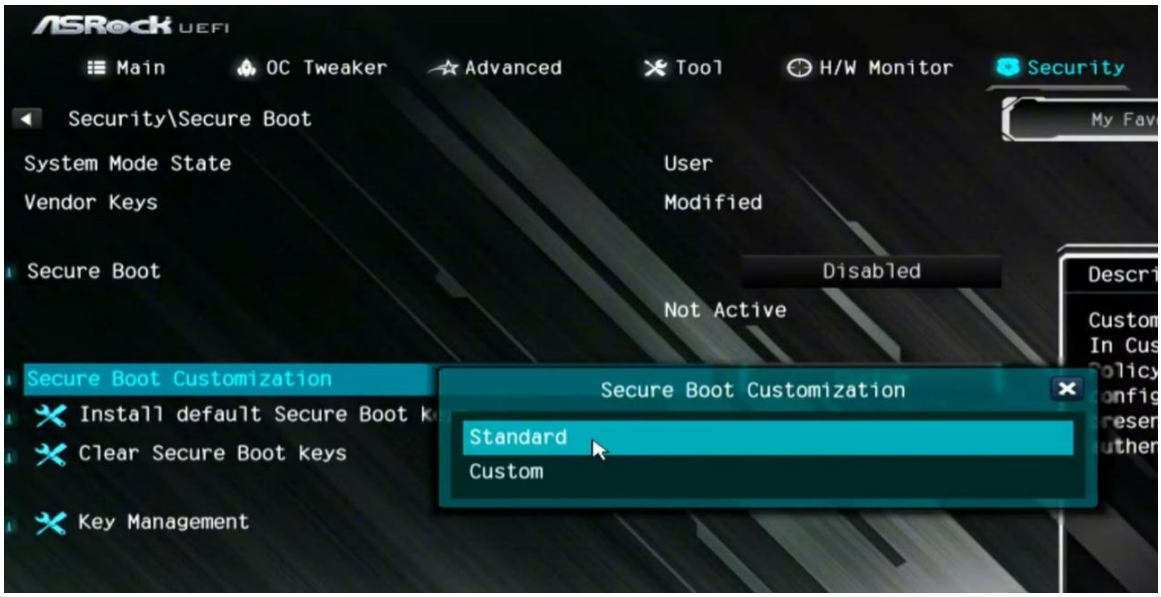
→ Stay in Security → Secure Boot.



→ Go to Secure Boot and change to Enabled.



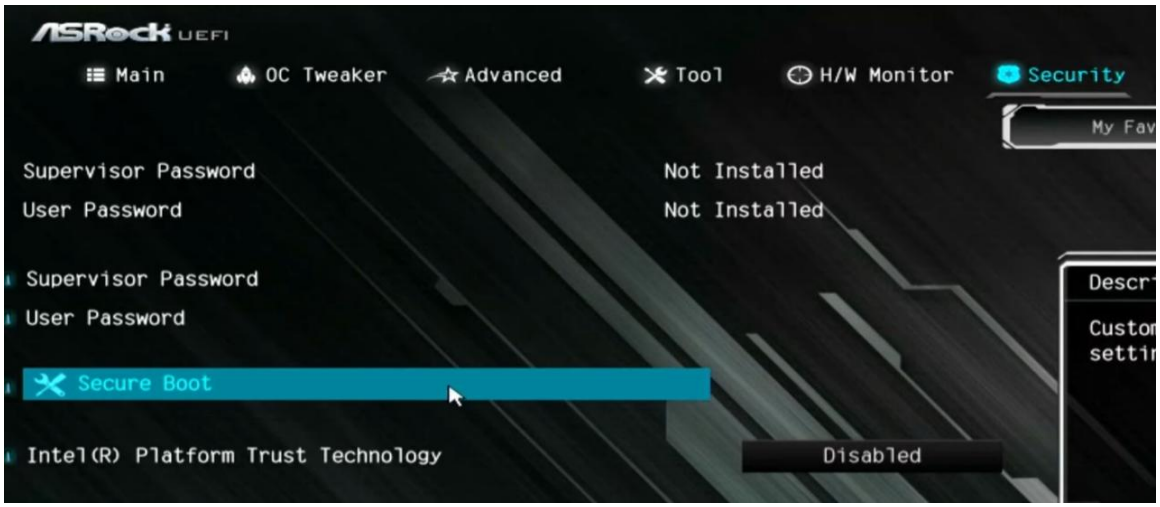
→ Go to Secure Boot Customization and change to Standard.



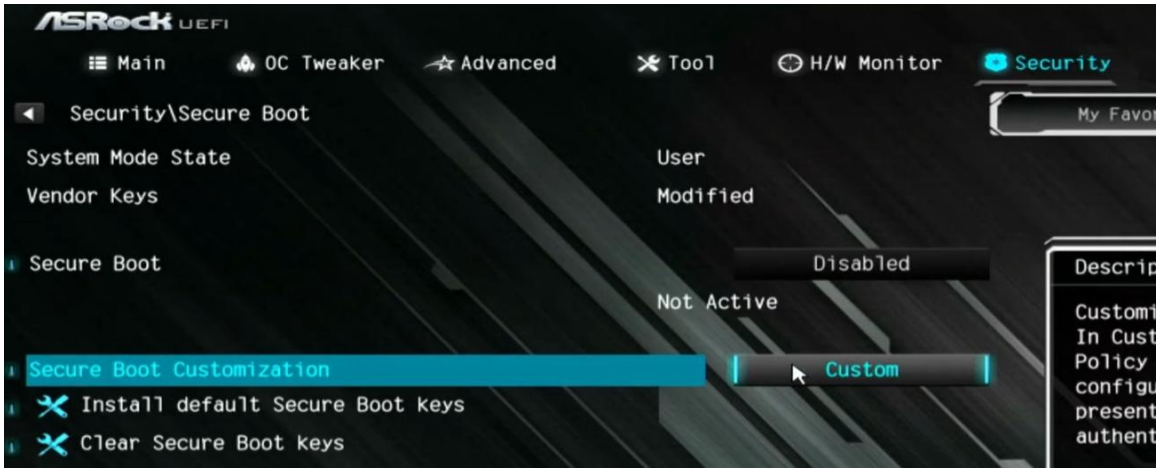
→ Press F10 to save and restart.

4 If it doesn’t work

→ Return to Security → Secure Boot.



→ Go to Secure Boot Mode and change to Custom.



→ Press F10 to save and restart.

5 Enable TPM — AMD (fTPM)

→ Go to Advanced → CPU Configuration.

→ Go to AMD fTPM switch and select AMD CPU fTPM (or Enabled).

→ Press F10 to save and restart.

6 Enable TPM — Intel (PTT)

→ Go to Security (or Advanced, depending on the model).

→ Go to Intel Platform Trust Technology (PTT) and change to Enabled.

→ Press F10 to save and restart.

7️⃣ Final tips and verification

→ Secure Boot requires the system drive to be in GPT format (not MBR) and a GPU with UEFI/GOP support.

→ If nothing works: use Load UEFI Defaults / Load Optimized Defaults (usually F9/F5) and repeat from step 2.

→ In Windows, confirm: Windows Security → Device Security → Security Processor Details (shows TPM 2.0).

🔒 Generic Guide – Secure Boot & TPM (Colorful / Mancer / Pichau)

(No images available; menu names may vary between models and BIOS versions.)

1️⃣ Enter the BIOS

→ Turn on or restart the PC.

→ As soon as the logo appears, press DEL (Delete) or F2 repeatedly.

→ 60% keyboard: use Fn + DEL/F2.

→ Inside the BIOS, press F7 to enter Advanced Mode (when available).

2️⃣ Set to UEFI (disable CSM)

→ Boot or Settings → Advanced → Windows OS Configuration.

→ BIOS CSM/UEFI Mode = UEFI (or Windows 10/11 WHQL Support = Enabled/UEFI on some models).

→ If CSM Support is present, set to Disabled.

→ Press F10 to save and return to the BIOS.

3️⃣ Secure Boot — first attempt (Standard)

→ Security/Boot → Secure Boot.

→ Secure Boot = Enabled.

→ Secure Boot Mode = Standard.

→ Press F10 to save and restart.

4️⃣ Secure Boot — if it doesn't work (Custom/Keys)

→ Go back to Security/Boot → Secure Boot.

→ Secure Boot Mode = Custom.

→ Enable Secure Boot Present → Hardware/OS Company, if available.

→ If it still doesn't work, try Maximum Security (when available).

→ Install the keys: Install Default Keys / Restore Factory Keys.

→ Press F10 to save and restart.

5️⃣ Enable TPM — AMD (fTPM)

→ Settings → Security → Trusted Computing.

→ Security Device Support = Enabled.

→ TPM Device Selection = AMD CPU fTPM.

→ Press F10 to save and restart.

6️⃣ Enable TPM — Intel (PTT)

→ Settings → Security → Trusted Computing.

→ Security Device Support = Enabled.

→ TPM Device Selection = PTT / Intel Platform Trust Technology.

→ Press F10 to save and restart.

7️⃣ Check in Windows

→ Win + R → tpm.msc → confirm TPM 2.0 is active.

→ Win + R → msinfo32 → check Secure Boot State = On.

8️⃣ If menus don't exist or don't appear

→ Update the BIOS to the manufacturer's latest official version.

→ Some entry-level models (especially Colorful) may not have Secure Boot/TPM in the BIOS.

→ In “generic” BIOS (Mancer/Pichau cases), names may differ; if the option doesn’t exist, it cannot be enabled.

→ If necessary, seek a professional to check BIOS/UEFI and the disk partition (GPT is required for Secure Boot).

9️⃣ Quick tip (GPT disk)

→ Secure Boot requires UEFI + system disk in GPT format.

→ If your disk is MBR, you will need to convert it to GPT (e.g., mbr2gpt) — recommended to have a professional do it.

Final Consideration

Correctly configuring **Secure Boot** 🔒 and **TPM** ensures compatibility with anti-cheat systems like **BlackBox** and **Black Security**, both essential for keeping competitive gameplay 🎯 fair and cheat-free. These features add an extra security layer, preventing unauthorized system modifications and protecting the integrity of online matches.

During the setup process, it's important to pay special attention to **disabling CSM** ⚠️. If your system drive is formatted as **MBR**, the PC may fail to boot or display video, requiring a conversion to **GPT**. It's also worth noting that some older motherboards do not support **TPM 2.0**, making full activation impossible.

This guide also reflects the practical expertise of companies like **P3ninha Optimizations**, which apply advanced system tweaks ⚙️, audio enhancements 🔊, and exclusive network optimization technology 🌐. These improvements deliver lower latency, faster server response times, and a stable, precise competitive experience — highly valued by professional and competitive players.

After completing the configuration:

- **Save BIOS changes using the F10 key** 💾.
- In Windows, go to **System Information** → **Secure Boot State** to confirm it shows as **On** ✅.

By following these steps, your system will be ready to meet the strict requirements of top anti-cheats, ensuring stability, security, and peak performance.