# Kích hoạt hoặc vô hiệu hóa Secure Boot thông qua tiện ích ASUS UEFI BIOS

Theo mặc định, Secure Boot được kích hoạt trên bo mạch chủ ASUS bằng UEFI BIOS. Tuy nhiên nếu muốn cài đặt dual-boot, bạn sẽ phải vô hiệu hóa Secure Boot đi. Trong bài viết dưới đây Quản trị mạng sẽ hướng dẫn bạn các bước vô hiệu hóa Secure Boot trên UEFI BIOS trên bo mạch chủ (motherboard) Asus X99-Deluxe.



## 1. Điều kiện tiên quyết cho Windows UEFI Mode: phân vùng GPT

Việc cài đặt Windows trên UEFI - nền tảng hệ thống yêu cầu kiểu phân vùng ổ đĩa cứng phải hỗ trợ chế độ UEFI Mode hoặc ít nhất là chế độ Legacy BIOS - chế độ tương thích.

Và nếu trên màn hình hiển thị thông báo lỗi dưới đây có nghĩa là máy tính của bạn được khởi động ở chế độ UEFI mode nhưng ổ đĩa cứng không hỗ trợ UEFI mode:

"Windows cannot be installed to this disk. The selected disk is not of the GPT partition style"



Phân vùng GPT trên ổ đĩa cứng được yêu cầu cho UEFI Mode. Ngoài ra điểm lợi thế của phân vùng GPT là người dùng có thể thiết lập ổ đĩa có kích thước lớn hơn 4 GB và có nhiều phân vùng hơn.

Cách đơn giản nhất để áp dụng phân vùng GPT trên ổ đĩa cứng của bạn là thông qua Command Prompt bằng cách sử dụng ổ đĩa cài đặt hoặc công cụ trên Widows.

# 2. Sử dụng Command Prompt để chuyển đổi ổ đĩa cứng thành phân vùng GPT

- Chèn ổ đĩa hoặc ổ USB Windows setup vào và khởi động máy tính của bạn ở chế độ UEFI.
- Sau khi khởi động từ Windows setup, nhấn tổ hợp phím Shift + F10 để mở cửa sổ Command Prompt.
- Tiếp theo mở công cụ disk partition tool bằng **diskpart**.

- Liệt kê và xác nhận ổ để format (định dạng) bằng list disk.
- Lựa chọn ổ đĩa để format và chuyển đổi thành GPT:

### select disk <disk number here>

#### clean

#### convert gpt

#### exit

• Đóng cửa sổ Command Prompt và tiếp tục.

```
windows) system32 icmd.exe - disk
Microsoft Windows [Version 10.0.10240]
X:\Sources>diskpart
 Aicrosoft DiskPart version 10.0.10240
 Copyright (C) 1999-2013 Microsoft Corporation.
On computer: MINWINPC
DISKPART> list disk
                             Size
                                                     Gpt
   Disk ### Status
                                      Free
                                                Dyn
                             465 GB
                                       465 GB
   Disk 0
            Online
   Disk 1
                               14 GB
             Online
                                          0 B
 DISKPART> select disk 0
 Disk 0 is now the selected disk.
 DISKPART> clean
 DiskPart succeeded in cleaning the disk.
 DISKPART> convert gpt
 DiskPart successfully converted the selected disk to GPT format.
  DISKPART>
```

# 3. Sử dụng Windows Partition Manager Tool để chuyển đổi ổ đĩa cứng thành phân vùng GPT

Ngoài ra bạn có thể chuyển đổi thành GPT mà không cần phải sử dụng Command Prompt bằng cách sử dụng công cụ Windows partition manager tool (công cụ quản lý phân vùng) từ EaseUS. EaseUS partition master có thể hỗ trợ bạn chuyển đổi ổ đĩa cứng thành GPT. Ngoài ra bạn có thể tạo, gộp, xóa phân vùng hoặc wipe partion. Ngoài ra công cụ cũng hỗ trợ bạn trong việc khôi phục dữ liệu trong trường hợp nếu dữ liệu bị xóa hoặc bị mất phân vùng.

## 4. Các bước sao lưu Existing Keys và vô hiệu hóa Secure Boot

- Chèn ổ USB vào máy tính của bạn.
- Khởi động lại máy tính và truy cập chế độ BIOS bằng cách nhấn phím DEL (hoặc sử dụng phím khác, chú ý trên cửa sổ hướng dẫn đầu tiên). Điều này để mở giao diện UEFI BIOS.
- Truy cập Advanced Mode (nhấn phím F7 hoặc phím chỉ định khác).

Immation         CPU Ter           > DELUKE         BIOS Ver. 1762           eRR Xecon(R) CPU IS-1650 v3 @ 3.500Hz           ext: 1500 Met:           mory: 32768 MB (DDM 2133MHz)	nperature 311C	CPU Core Voltage 1.008 V Motherboard Temperature 28°C	EZ System Tuning Click the icon to specify your preferred system settings for an improved system performance of a power-saving system cerviconment. Cuter
RAM Status Mal At: Conser 868 2133MHz Mal A2: KVA Mal B2: Conser 868 2133MHz Mal B2: NA Mal D2: Conser 868 2133MHz Mal C1: Conser 868 2133MHz Mal C1: Conser 868 2133MHz	SATA Informat P1: Sensung SSD 8 P2: NA P3: NA P4: NA P5: NA P5: NA	tion Iso EVO 500GB (500.1GB)	Keego Soung     Kormal     Normal     Subscription     Korea and drag the items.     Switch all
IMML D2: NVA KM.P P Disabled AN Profile D CPU FAN NVA NVA	Intel Rapid Sto On CPU FAN	vrage těchnology off	Windows Boot Manager (P1: Semsung SSD asis EVO Scocel)
DUAD FAN DUAD FAN DUA FAN DUA FAN DUA FAN DUAF FAN NAA DUA FAN DUAF FAN NAA			P1: Semourg SSD 850 EVO 50008

• Truy cập tùy chọn Secure Boot nằm dưới mục Boot.

BIOS Information BIOS Version Build Date PCH Stepping EC1 Version EC2 Version ME Version	1702 04/10/2015 5/C2 MBEC-X99-0423 RGE2-X99-0204 9.1.10.1005	CPU Frequency Temperature 3500 Mitz 33°C BCLX Core Voltage 100.0 Mitz 1,008 V Reto 35x
CPU Information Intel(R) Xeon(R) CPU ES-1650 v3 @ 3.50GHz Speed Memory Information Total Memory Memory Frequency	3500 MHz 32768 MB 2133 MHz	Memory Prequency Vol. CHAB 2133 Mile: 1,209 V Capacity Vol. CHCD 32768 MB 1,209 V
System Language System Date Sustan Tima Choose the system default language	06/23/2015 06/23/2015 00:42:25	• 12V -5V 12.066 V 5.046 V •3.344 V

 Hãy chắc chắn rằng lựa chọn đúng OS Type, sau đó truy cập Key Management.

×uto *	
	Frequency Temperatur
3 sec 👻	3500 MH2 32*C
Enabled *	BCLK Core Voltage 100.0 MHz 1.008 V
Enabled -	Ratio
Enabled -	35x
Force BIOS +	Memory
Timmediate	Frequency Vol. CHAB 2133 MBr 1,206 V
Disabled +	Capacity Vol. CHCD
EZ Mode +	32768 MB 1,206 V
	Voltage
	12V +5V 12.096 V 5.040 V
	Enabled * Enabled * Enabled * Force BIOS * Immediate * Disabled * EZ Mode *

• Chọn Save Secure Boot Keys rồi nhấn Enter.

My Favorites Main Al Twea	ker Advanced Monitor <u>Boot</u>	Tool Exit	Hardware Monito
- Boot/Secure Boot			CPU
Secure Boot state Platform Key (PK) state	Enabled Unloaded		Frequency Temperature 3500 MHz 32*C
OS Type	Windows UE	FI mode	BCLK Core Voltage 100.0 MHz 1.008 V
> Key Management			Ratio 35x
			Memory
	₽		Frequency Vol. CHAB 2133 MHz 1.206 V
			Capacity Vol_CHCD 32768 MB 1.209 V
			Voltage
			+12V -5V 12,096 V 5,040 V
Mindows UER mode): Execute the Microso other Microsoft secure boot compliant ope (Other OS): Select this option to get the opt non-compliant operating systems.	ft secure boot check. Only select this option when booting rating systems. mized functions when booting on Windows non-UEFI mod	on Windows UEFI mode or le and Microsoft secure boot	+3.3V 3.344 V

• Lựa chọn ổ USB khi được hỏi Select a File System.

				TOOL EX	at .	Hardw	are Monite
← Boot\Secure Boot\Key Management						CPU	
> Clear Secure Boot Keys					1	Frequency 3500 Mar	Temperatu
➤ Save Secure Boot Keys			2400		<b>MARKAGENE</b>	artis	are
PK Management			Loaded	11		100.0 MHz	1.008 V
> Delete PK					Ta Colorado	Ratio	
> Load Default PK						35x	
KEK Management			Loaded			Memory	
> Delete KEK		A				Frequency	Vol. CHAD
► Load Default KEK						2133 MHz	1.209 V
► Append Default KEK						Capacity 32768 MB	1209 V
DB Management			Loaded				
> Delete the db						Voltage	
> Load Default db						+12V 12.096 V	45V 5.040 V
Save all the secure boot keys to an LISB store	in dadea					+1.3V	
C an Use stora	ta device.					3.344 V	

• 4 key có tên PK, KEK, DB và DBX sẽ được lưu vào ổ USB.

escandor 00:45°   ⊕	English 🗇 MyFavorite(F3) 🕉 Qfan Controk(F6) 🛇 EZ Turning Wizard(F11) 🕞	Quick Note(F9) 2 Hot Keys
My Favorites Main	A Tweaker Advanced Monitor Boot Tool Exit	Hardware Monitor
e BootiSecure BootiKey Mana		CPÚ
➤ Clear Secure Boot Keys		Stresponcy Tomperature 3500 MHz 3310
• Cum Canina Boat Kaur	Select a File System	
	Acpi(a0341d0, 0)\PCI(1F[2)\DevicePath(Type 3, SubType 18)HD(Part2, Sig ?) Acpi(a0341d0, 0)\PCI(1F[2)\DevicePath(Type 3, SubType 18)HD(Part4, Sig ?) Acpi(a0341d0, 0)\PCI(1A[0)\US8(0,0)\US8(2,0)\HD(Part1, Sig ?)	
	43	
	OK Cancel	
		Last Modified   ErMode(77)]-2

Xóa Platform Key (PK) để vô hiệu hóa Secure Boot (lưu ý không xóa các key khác).

VESLUS UEFI BIOS Unity - Adv	anced Mode		Sale Partie Sale
Second 00:45			Durk Notecron 12 Junit stays
My Favorites Main Ai Ty	veaker Advanced Monitor		
- Doot/Secure Bost/Key Management			
* clear Secure Root Keys			
Save Sa	rurity Key/Database		
Jave Je	(c) read to dick!		
	(a) saved to disk!		
	N		
		OK Cancel	

• Lưu và khởi động lại để áp dụng thiết lập (thường sử dụng phím F10).



### 5. Khôi phục key và kích hoạt Secure Boot

- Thực hiện theo các bước từ 1 đến 5 ở phần trên. Sử dụng ổ USB có chứa sao lưu các key.
- Truy cập Load Default PK rồi nhấn Enter. Và bạn sẽ có 2 tùy chọn để thiết lập key mới.

My Favorites Main	Ai Tweaker Advanced	Monitor Boot	Tool Exit	Hardware Monito
Boot\Secure Boot				СРО
Secure Boot state Platform Key (PK) state		Disabled Unloaded		Frequency Temperatur 3500 MHz 33°C
OS Type		Other O	s	BCLK Core Voltage 100.0 MHz 1.008 V
Key Management				Ratio 35x
				Memory
		ß		Frequency         Vol. CHAB           2133 MHz         1.206 V           Capacity         Vol. CHCD           2004 Line         1.206 V
				Voltage
				120 500 V 5.040 V
Windows UEFI mode): Execute other Microsoft secure boot co [Other OS]: Select this option to non-compliant operating syste "The Microsoft secure boot co	the Microsoft secure boot check. Only se propliant operating systems. 9 get the optimized functions when boot rms.	elect this option when boo ing on Windows non-UEFI	iting on Windows UEFI mode o mode and Microsoft secure bo	* 3.3V 3.344 V iot

- Chọn Yes để load key mặc định. Sau khi hoàn tất, lưu lại cấu hình và khởi động lại để kích hoạt Secure Boot.
- Chọn No để load sao lưu các key:

My Favorites Main	u rweaker	Advanced	Monitor	Boot	Tool	Exit	Hard	Are Monito
<ul> <li>Boot\Secure Boot\Key Managem</li> </ul>	ent						CPU	one morator
Install Default Secure Boot Keys							Frequency	Temperature
Save Secure Boot Keys						State of the	3500 MHz	32*C
PK Management				Inloaded			BCLK	Core Voltage
Delete PK			Service P	Contraction of the		ALC: NOT ALC: NOT	100.0 1042	1.008 V
Load Default PK							35x	
KEK Management	Service State		1	oaded	220200	STREET, STREET, ST	Mamoni	
> Delete KEK			N				memory	hetraine
Load Default KEK			45			Contraction of	2133 MHz	1.209 V
Append Default KEK							Copilcity	Vol_CHCD
OB Management							32768 MB	1.212 V
> Delete the db			0	Moed			Voltage	
> Load Default db							+12V 12.096 V	+5V 5.040 V
Select yes to load the system defau (Yes): Load the default PK. [No]: Load the PK from an USB stor	k PK(platform key	) or select no to loa	id a downloaded	PK from an US	iB storage d	wke.	+3.3V 3.344 V	

• Chọn ổ USB có chứa các file sao lưu.



• Lựa chọn file để khôi phục (trong trường hợp này là PK).

Install Default Secure Boot				
S OF STITLE ROAT DOVE	Select File	CHOICE STREET,		
	<.fseventsd> <system information="" volume=""> &lt;.Trashes&gt; &lt;.Spotlight-V100&gt;</system>			
	KEK db dbx Trashes	¢,		
		ок	] Cancel	]

• Xác nhận là UEFI Secure Variable.



• Xác nhận bạn muốn cập nhật (update) file PK.

and a substance of the substance	e san avakunar	stavil oreal	Manitor	Ale of	Topl	Exit		International International
	Set New Key							
	Update 'PK' from select	ted File 'PK'?						
			~~					
					-	ALL ROOM	-	
				N.		No		
			0	ĸ	Car	icel		

 Lưu lại thay đổi và tiến hành khởi động lại. Secure Boot sẽ được kích hoạt.