

EVE-NG Documentation

Table of Contents

How to enable Windows 11 Virtualization	2
BIOS Settings	2
Disable Memory Integrity	2
Disable MS Windows 11 features related for Hyper-V	3
Disable MS Windows 11 Hyper-V service by CLI	3
Turn OFF Virtualization-based-Security (important)	4
Verify your Windows 11 virtualization settings	4

© EVE-NG LTD

The information contained in this document is the property of EVE-NG Limited

The contents of the document must not be reproduced or disclosed wholly or in part or used for purposes other than that for which it is supplied without the prior written permission of EVE-NG Limited.

How to enable Windows 11 Virtualization

BIOS Settings

 First you must be sure if your CPU supports virtualization and it is enabled in the BIOS. Different vendors and BIOS will have different screen and setup options, but logic virtualization settings are same. Virtualization must be set as ON. Below is example for Lenovo X1 Carbon Laptop BIOS.

ThinkPad	← Virtualization	
	> Kernel DMA Protection	On OFF
Setup	> Intel(R) Virtualization Technology	On ON
<table-cell> Main</table-cell>	> Intel(R) VT-d Feature	On ON
鴪 Config	> Enhanced Windows Biometric Security	Off OFF
② Date/Time		
🔒 Security		
⊥ Startup		
🗘 Restart		
Lenovo		

Disable Memory Integrity

2. Disable Windows 11 Memory Integrity option:

It's located as following in Windows 11:

Settings -> Privacy & security -> Windows Security -> Device security -> Core isolation -> Memory integrity.

	Disa	able	e it/	OF	F.
--	------	------	-------	----	----



Disable MS Windows 11 features related for Hyper-V

- 3. Go to Control Panel/All Control Panel Items/Programs and features/Turn Windows Features on or off.
 - 3.1. **Disable (uncheck)** Hyper-V, Windows Machine Platform and Windows Hypervisor platform



Disable MS Windows 11 Hyper-V service by CLI

4. RUN CMD as administrator or Powershell to disable MS hypervisor service.

bcdedit /set hypervisorlaunchtype off

Close the command prompt after executing the commands and restart the Windows 11 system.

Turn OFF Virtualization-based-Security (important)

- 5. Process to turn off virtualization-based Security:
 - 5.1. Use Windows 11 Search and find Group policy editor (Windows 11 Pro only), Home edition is required to make settings manually via regedit. *VM Ware kbit link below.*

Q Group policy	
All Apps Documents Web More ~	o₩U
Best match	
Edit group policy Control panel	
Search the web	Edit group policy
Ø Group policy - See web results >	Control panel

- 5.2. Go to Local Computer Policy > Computer Configuration > Administrative Templates > System
- 5.3. Double Click on Device Guard on the right-hand side to open.
- 5.4. Double Click on "Turn on Virtualization Security" to open a new window
- 5.5. It would be "Not Configured", Select "Disable" and click "Ok"
- 5.6. Close the Group Policy Editor.

5.7. Restart the sy	vstem			
Local Group Policy Editor			- 🗆 X	
File Action View Help				
🗢 🔶 📶 📑 📓 🖬 🝸				
Access-Denied Assistance	Device Guard			ſ
App-V App-V Audit Process Creation Credentials Delegation Device Guard Device Guard Device Health Attestation Service	Turn On Virtualization Based Security Edit <u>policy setting</u>	Setting Deploy Windows Defender Application Turn On Virtualization Based Security	Control Disabled Disabled	
	Requirements: At least Windows Server 2016, Windows 10 Description: Specifies whether Virtualization Based Security is enabled.	Turn On Virtualization Based Security	Previous Setting	- D X
Early Launch Antimalware Enhanced Storage Access File Classification Infrastructure File Share Shadow Copy Provider Filesystem Folder Redirection Group Policy	Virtualization Based Security uses the Windows Hypervisor to provide support for security services. Virtualization Based Security requires Secure Boot, and can optionally be enabled with the use of DMA Protections. DMA protections require hardware	Not Configured Comment: Enabled Disabled Supported on:	t least Windows Server 2016, Windows 10	* * *
Internet Communication Managemer Si iSCSI KDC	support and will only be enabled on correctly configured devices.	Options:	Help:	
2 setting(s)	Extended (Standard/ Uvvice Encryption Support Hyper-V - VM Monitor M Hyper-V - Second Level	Select Platform Security Level: Virtualization Based Protection of Code Int	Specifies whether Virtualization E Virtualization Based Security use provide support for security servi requires Secure Boot, and can op DMA protections DMA protections	lased Security is enabled. Is the Windows Hypervisor to ices. Virtualization Based Security tionally be enabled with the use of the require hardware support and
	Hyper-V - Second Level /	~	will only be enabled on correction	configured devices

Verify your Windows 11 virtualization settings

6. To verify if your Windows has disabled Virtual machine security:

msinfo32/system

Administrator: Command Prompt Microsoft Windows [Version 10.0.22631.3155] (c) Microsoft Corporation. All rights reserved. C:\Windows\System32>msinfo32/system C:\Windows\System32>

Output MUST show:

💐 System Information		
File Edit View Help		
System Summary Hardware Resources Components Software Environment	ItemInstalled Physical Memory (RAM)Total Physical MemoryAvailable Physical MemoryTotal Virtual MemoryAvailable Virtual MemoryPage File SpacePage FileKernel DMA ProtectionVirtualization-based securityWindows Defender Application Control policyWindows Defender Application Control user mode policyDevice Encryption Support	Value 32.0 GB 31.7 GB 22.3 GB 23.0 GB 2.00 GB C:\pagefile.sys On Not enabled Enforced Off Meets prerequisites

Reference to: https://kb.vmware.com/s/article/2146361