How to enable or disable Device Guard on Windows 10

Device Guard is a combination of enterprise-related software and hardware security features, when configured together, locks the device to run only trusted applications that you specify in the code integrity policy. .

Device Guard is a combination of enterprise-related software and hardware security features, when configured together, locks the device to run only trusted applications that you specify in the code integrity policy. . If the application is not trusted, it will not be able to run. With hardware that meets the basic requirements, that means that even if an attacker can gain control of the Windows kernel, they cannot run malicious executable code. With the right hardware, Device Guard can use the new virtualization-based security in Windows 10 to isolate the Code Integrity service from Microsoft Windows. In this case, the Code Integrity service runs in the same folder as the Windows virtualized protected container.

This tutorial will show you how to enable or disable security based on Device Guard virtualization on Windows 10 Enterprise and Windows 10 Education PCs.

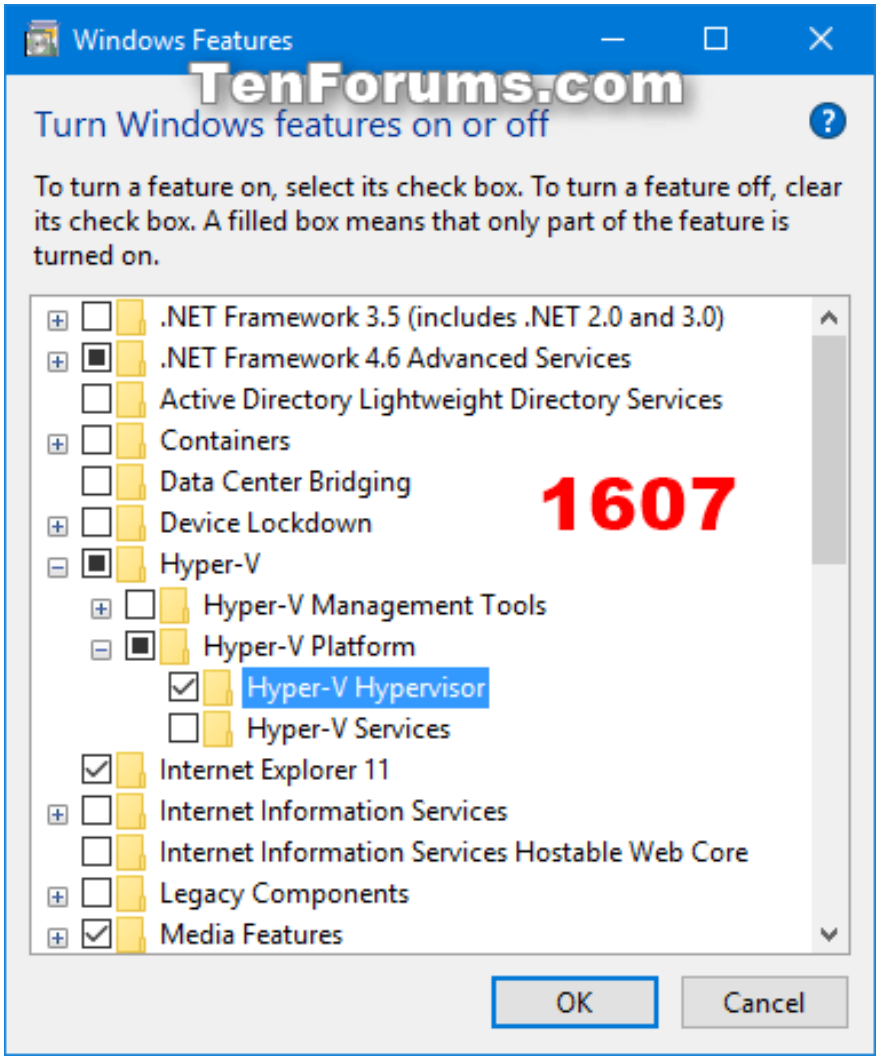
You must log on as an administrator to enable or disable Device Guard.

1. How to open Windows Security in Windows 10
2. How to turn on Tamper Protection for Windows Security on Windows 10
3. Enhance Windows 10 security with Exploit Protection

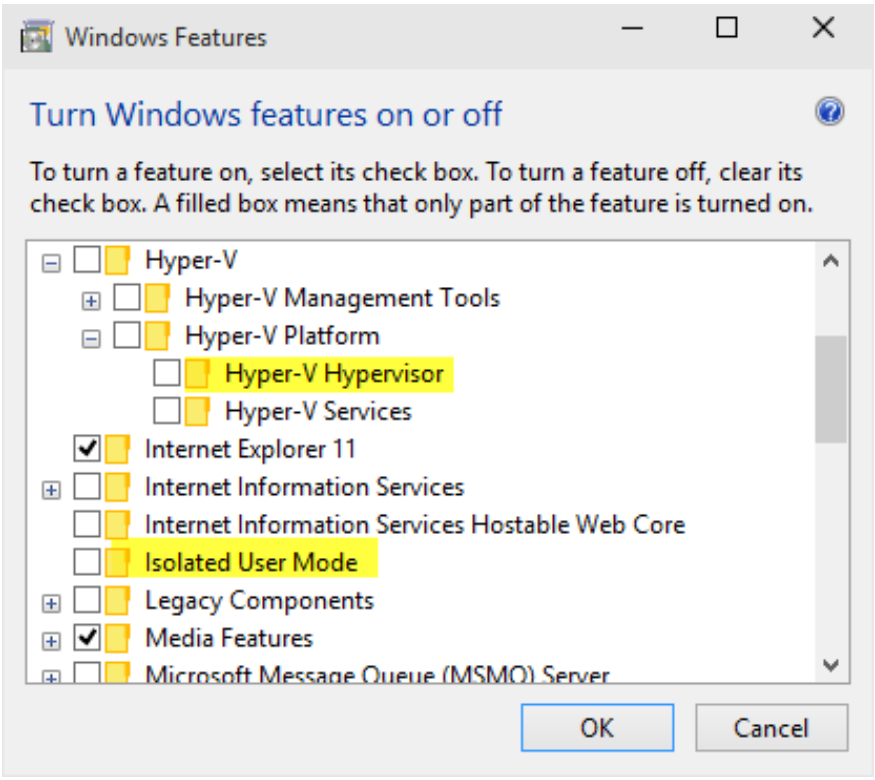
How to enable or disable Device Guard

Step 1 . Open the Windows Features.

In Windows 10 Enterprise / Education version 1607 or later, select **Hyper-V Hypervisor** in **Hyper-V** and click **OK** .



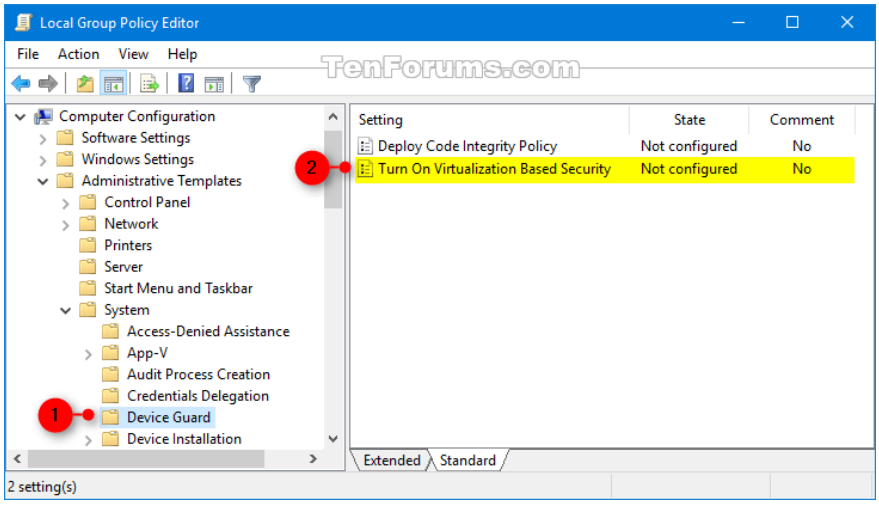
In Windows 10 Enterprise / Education versions before version 1607, select **Hyper-V Hypervisor** in Hyper-V, select **Isolated User Mode** and click **OK** .



Step 2 . Open Local Group Policy Editor.

Step 3 . Navigate to the following key in the left pane of Local Group Policy Editor.

```
Computer ConfigurationAdministrative TemplatesSystemDevice Guard
```



Step 4 . In the right pane of Device Guard in the Local Group Policy Editor, double-click the **Turn On Virtualization Based Security policy** to edit it.

Step 5 . Follow Step 6 (turn on) or Step 7 (off).

Step 6 . To activate Device Guard

1. Select **Enabled** .
2. In Options, select **Secure Boot** or **Secure Boot and DMA Protection** in the Select Platform Security Level drop-down menu.

Note: The Secure Boot (recommended) option provides secure boot with multiple protections supported by specific computer hardware. A computer with an input / output memory manager (IOMMUs) will have a safe boot with DMA protection. A computer without IOMMUs will only activate secure boot.

Secure Boot with DMA will enable secure booting and VBS only on computers that support DMA, ie computers with IOMMUs. With this setting, any computer without IOMMU will not have VBS protection (hardware-based), although it can enable code integrity policies.

1. In Options, select **Enabled with UEFI lock** or **Enabled without lock** in the Virtualization Based Protection drop-down menu of Code Integrity.

Note: Enabled with UEFI lock option ensures Virtualization Based Protection of Code Integrity is not disabled remotely. To disable this feature, you need to set up Group Policy Disabled as well as delete the security for each computer with the current user to delete the configuration on UEFI.

Option **Enabled without lock** for Virtualization Based Protection of Code Integrity is remotely disabled using Group Policy.

1. If you wish, you can also activate Credential Guard by selecting **Enabled with UEFI lock** or **Enabled without lock** in the drop-down menu Credential Guard Configuration.

Note: Enabled with UEFI lock option ensures Credential Guard is not disabled remotely. To turn off this feature, you must set Group Policy to Disabled as well as delete the security function in each computer with the current user to delete the configuration in UEFI.

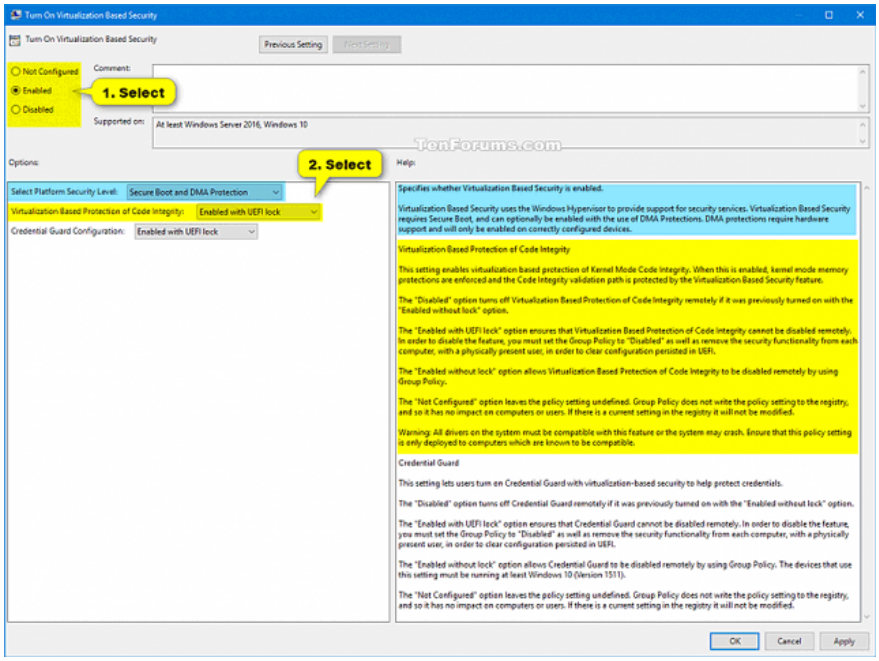
Enabled without lock option allows Credential Guard to be turned off remotely using Group Policy. Devices using this installation need to run on the operating system from Windows 10 (Version 1511) or later.

1. Go to Step 8.

Step 7 . To disable Device Guard

Select **Not Configured** or **Disabled** , click **OK** and go to Step 8.

Note : Not Configured is the default setting.



Step 8 . Close Local Group Policy Editor.

Step 9 . Restart the computer to apply changes.

I wish you all success!

You finished reading the article "**How to enable or disable Device Guard on Windows 10**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

© 2019 TipsMake.com