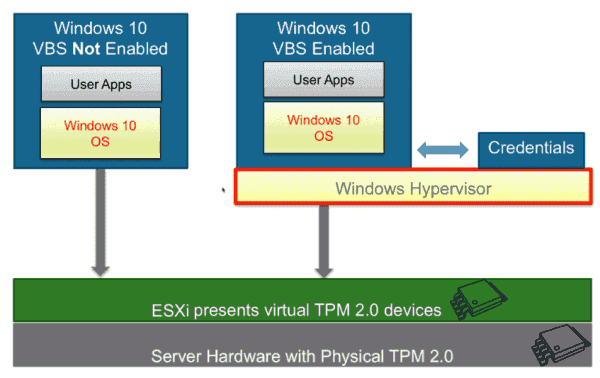
What is Virtualization-based Security (VBS)?[^](https://4sysops.com/archives/enable-windows-10-virtualization-based-security-vbs-for-vsphere-6-7/#Content-bal-title)

VBS uses hardware and software virtualization features to enhance Windows system security by creating an isolated, hypervisor-restricted, specialized subsystem.

Basically, Microsoft is using a Windows role (or component) called the Hyper-V role, which boots the OS. This hypervisor allows Microsoft to isolate some sensitive information in places that would normally be accessible to the OS. Here we can think of cached credentials and such things.

Most modern systems have a Trusted Platform Module (TPM) 2.0 device built into the hardware. However, someone had to do it in software. And this is the goal. To give you an idea, here is a screenshot from a VMware blog post.

*[](https://4sysops.com/wp-content/uploads/2019/04/Microsoft-VBS.png)*

*Microsoft VBS*

As you can see, the Windows 10 virtual machine (VM) has a hypervisor role active and has the credentials stored elsewhere.

* MSI
* MSIX
* EXE
* APP-V

What are the restrictions on VBS-enabled VMs?[^](https://4sysops.com/archives/enable-windows-10-virtualization-based-security-vbs-for-vsphere-6-7/#Content-bal-title)

VBS is only usable on Windows 10 and Windows Server 2016, and vSphere features exist that are not compatible with VBS:

* VMware Fault Tolerance (FT)
* vSphere PCI passthrough
* vSphere hot add for CPU or memory

What are the vSphere requirements for VBS?[^](https://4sysops.com/archives/enable-windows-10-virtualization-based-security-vbs-for-vsphere-6-7/#Content-bal-title)

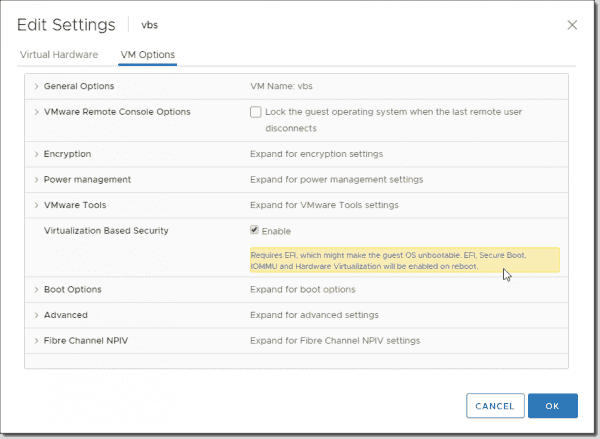
As mentioned above, VBS is only available as of vSphere 6.7. The requirements for working with VBS are:

* A VM with virtual hardware 14
* Hardware virtualization and an input/output memory management unit (IOMMU) exposed to the VM
* Secure boot enabled
* EFI firmware
* 64-bit CPU
* Intel VT-d or AMD-Vi ARM64 system memory management units (SMMUs)
* TPM 2.0

How do you enable VBS?[^](https://4sysops.com/archives/enable-windows-10-virtualization-based-security-vbs-for-vsphere-6-7/#Content-bal-title)

In the VMware vSphere client, first connect to vSphere and select the VM for which you want to enable VBS.

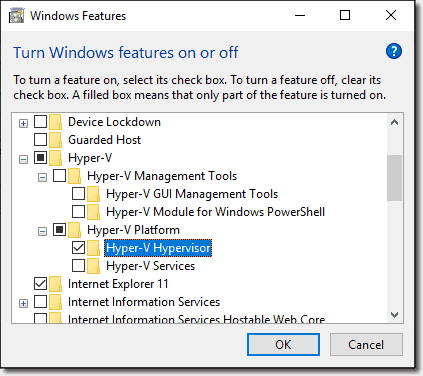
1. Shut down the VM and tick the **Enable** box next to **Virtualization Based Security** under VM Options.

*[](https://4sysops.com/wp-content/uploads/2019/04/Enabling-VBS.png)*

*Enabling VBS*

**Note**: *The VM has to be booting EFI (not BIOS) to satisfy the requirements. If you are creating new Windows 10 or Windows 2016 VMs, you should make sure you are selecting UEFI firmware before installing. After installing the system, it is pretty difficult to switch.*

And once the VM is up and running, we'll need to activate the Hyper-V role. You can do this through a simple command **appwiz.cpl**, which automatically brings up the window where we select Add/Remove **Turn Windows features on and off**. Once there, we can look for the Hyper-V section and check the box **Hyper-V Hypervisor**.

*[](https://4sysops.com/wp-content/uploads/2019/04/Enabling-the-Hyper-V-Hypervisor.png)*

*Enabling the Hyper V Hypervisor*

If you want to add a Hyper-V role on Windows Server 2016, you'll use the **Add roles and features** wizard within your Server Manager.

Once you're done, it'll ask you to **reboot the system**.

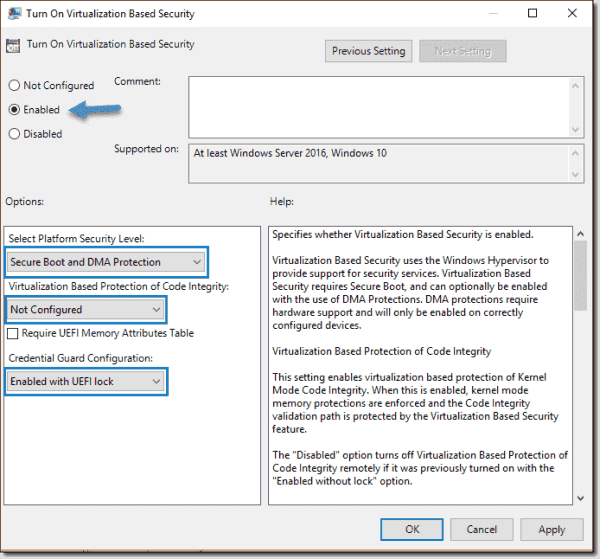
Let's continue after the VM comes up.

1. In the VM, open **gpedit.msc** and browse to:

**Computer Configuration > Administrative Templates > System > Device Guard > Turn On Virtualization Based Security**. Set it to **Enable** and configure the options as follows:

* Select Platform Security Level: Secure Boot and DMA Protection
* Virtualization Based Protection of Code Integrity: Enabled with UEFI lock
* Credential Guard Configuration: Enabled with UEFI lock

If you want to be able to turn off Windows Defender Credential Guard remotely, choose **Enabled without lock**.

*[](https://4sysops.com/wp-content/uploads/2019/04/Credential-Guard-configuration.png)*

*Credential Guard configuration*

If you want to activate VBS for multiple systems, you can do this via Group Policy in your domain.