Windows 11 Support on vSphere

Table of contents

Windows 11 Support on vSphere

Introduction

The goal of this article is to act as a single destination to guide you through the requirements needed to run Windows 11 virtual machines on vSphere.

Windows 11 requires TPM 2.0. Running Windows 11 as a virtual machine requires a virtual Trusted Platform Module to be present. For more details on Windows 11 requirements see, https://docs.microsoft.com/en-us/windows/whats-new/windows-11-requirements .

What is a virtual TPM device? Check out the information we have on vTPMs in vSphere.

Configuring vSphere to support Windows 11

Virtual TPM devices require vSphere to be configured with a Key Provider. This is a prerequisite requirement before you can create a new VM with a vTPM device or add a vTPM device to an existing VM. In vSphere 8 and vSphere 7 this can be a Native Key Provider or an external third party key provider. (Native Key Provider requires vSphere 7 U2 or later).

See the documentation links below to configure your respective version of vSphere with an appropriate key provider. The procedure for configuring vSphere to support Windows 11, will depend on which version of vSphere you are running. **Please take care to follow the procedure for your version of vSphere.**

Important: Adding a vTPM device requires a Key Provider, and the virtual machine "home" files are encrypted (memory, swap, NVRAM files). You are not required to encrypt the virtual machine disk files. vTPM and full VM Encryption are separate features. A vTPM does not require a physical Trusted Platform Module (TPM) 2.0 chip to be present on the ESXi host. However, if you want to perform host attestation, an external entity, such as a TPM 2.0 physical chip, is required. See Securing ESXi Hosts with Trusted Platform Module.

For more information, including an extensive Q&A on virtual TPMs, visit https://core.vmware.com/vtpm.

---

vTPM documentation for vSphere 8

- Configuring and Managing vSphere Native Key Provider
- Configuring and Managing a Standard Key Provider
- Securing Virtual Machines with Virtual Trusted Platform Module
- Virtual Machine Encryption Interoperability

vTPM documentation for vSphere 7

- Configuring and Managing vSphere Native Key Provider
- Configuring and Managing a Standard Key Provider
- Securing Virtual Machines with Virtual Trusted Platform Module
- Virtual Machine Encryption Interoperability

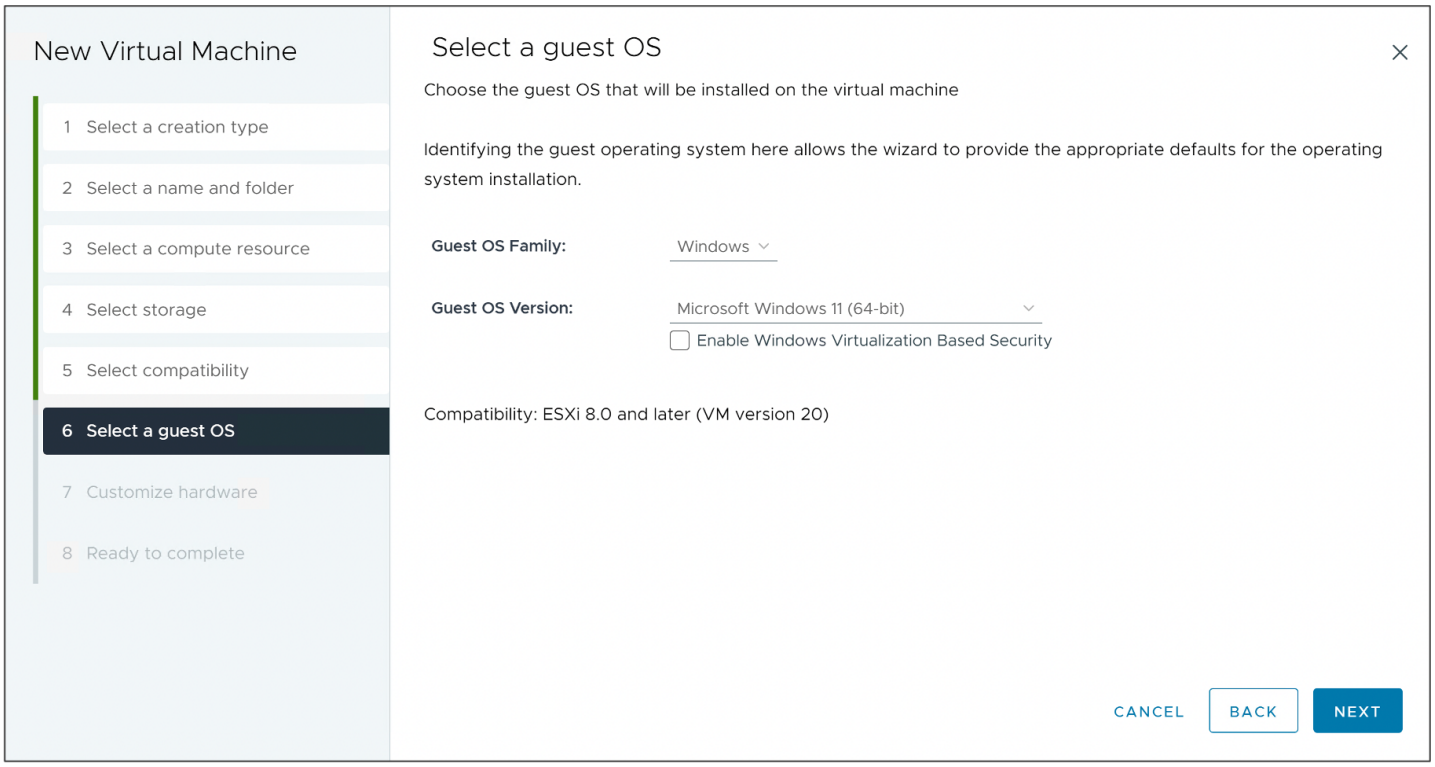
Windows 11 on vSphere

vSphere 8 and vSphere 7 support Windows 11. This section explains how to create a new VM to meet the requirements for Windows 11 for each vSphere release.

Installing Windows 11 in a Virtual Machine on vSphere 8

Installing Windows 11 in a virtual machine on vSphere 8 is almost identical to installing previous versions of Windows. The change is that Windows 11 requires a virtual TPM device to be present in the virtual machine.

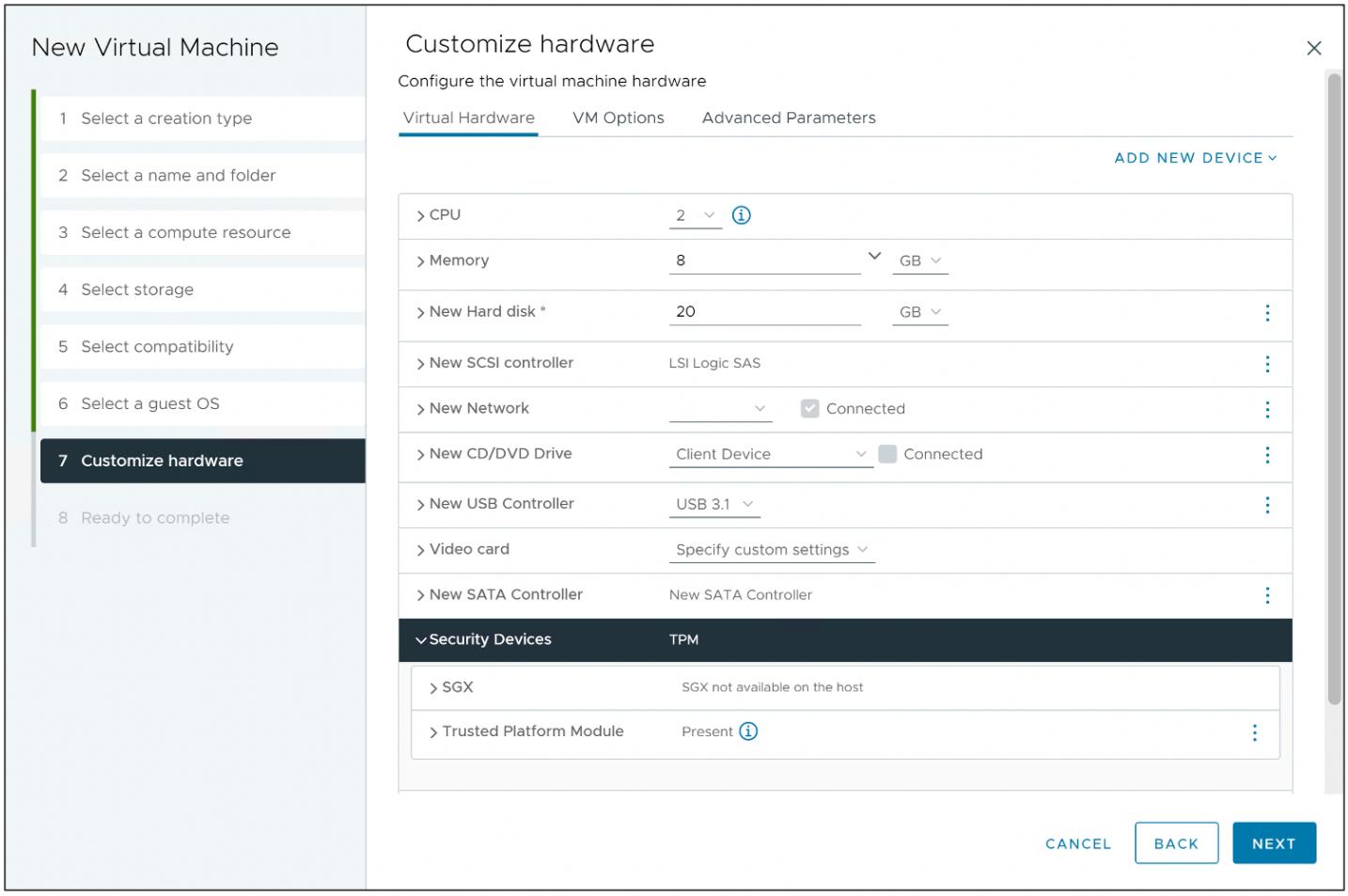
When creating a new virtual machine, using the vSphere Client, select virtual machine compatibility with ESXi 8.0 and later (hardware version 20) and choose Microsoft Windows 11 (64-bit) as the Guest OS Version.



Note: If you see the following warning, it means you do not have a key provider configured. Configure a vSphere Native Key Provider or Standard Key Provider.

```
Microsoft Windows 11 (64-bit) requires a Virtual TPM device, which cannot be added to this virtual machine because the Sphere environment is not configured with a key provider.
```

A Trusted Platform Module device is added by default during the new VM creation wizard.



Complete the new virtual machine wizard as normal and you are ready to install Windows 11.

See the VMware Guest Operating System Customization Matrix and the Windows 11 Guest Operating System installation guide for more details.

Note: The recommended choice for virtual storage controller is VMware Paravirtual SCSI (PVSCSI).
Refer https://kb.vmware.com/s/article/84200 to add the PVSCSI driver to Windows ISO or provide the driver to Windows during installation by following process mentioned in the section "*To install PVSCSI drivers through CD/DVD drive (Recommended)*" of KB https://kb.vmware.com/s/article/1010398.

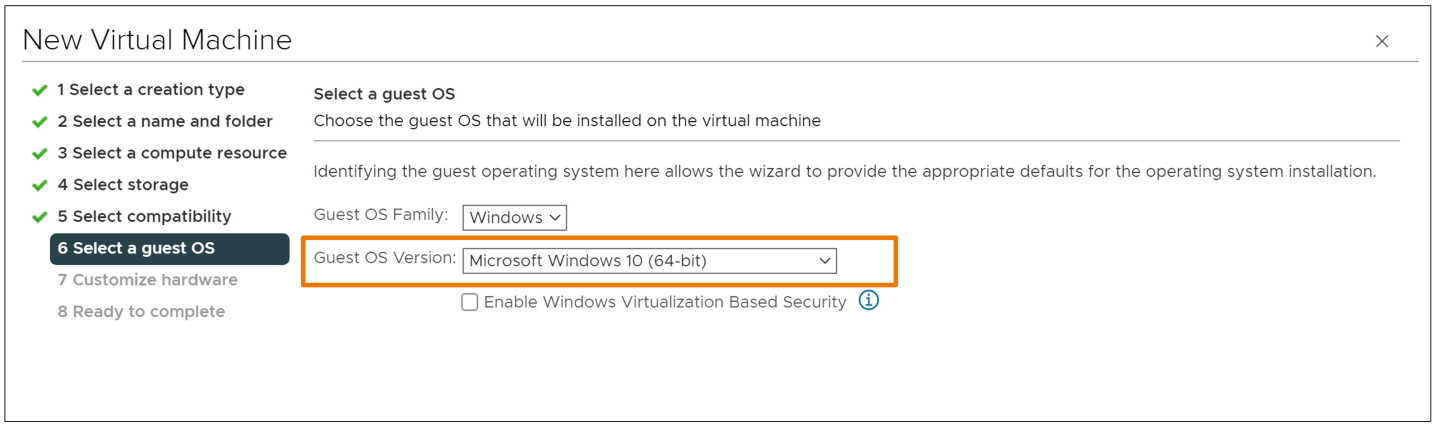
Windows 11 22H2 version includes VMware pvscsi drivers as part of the default Windows installation media!

Windows 11 Inbox VMware drivers.

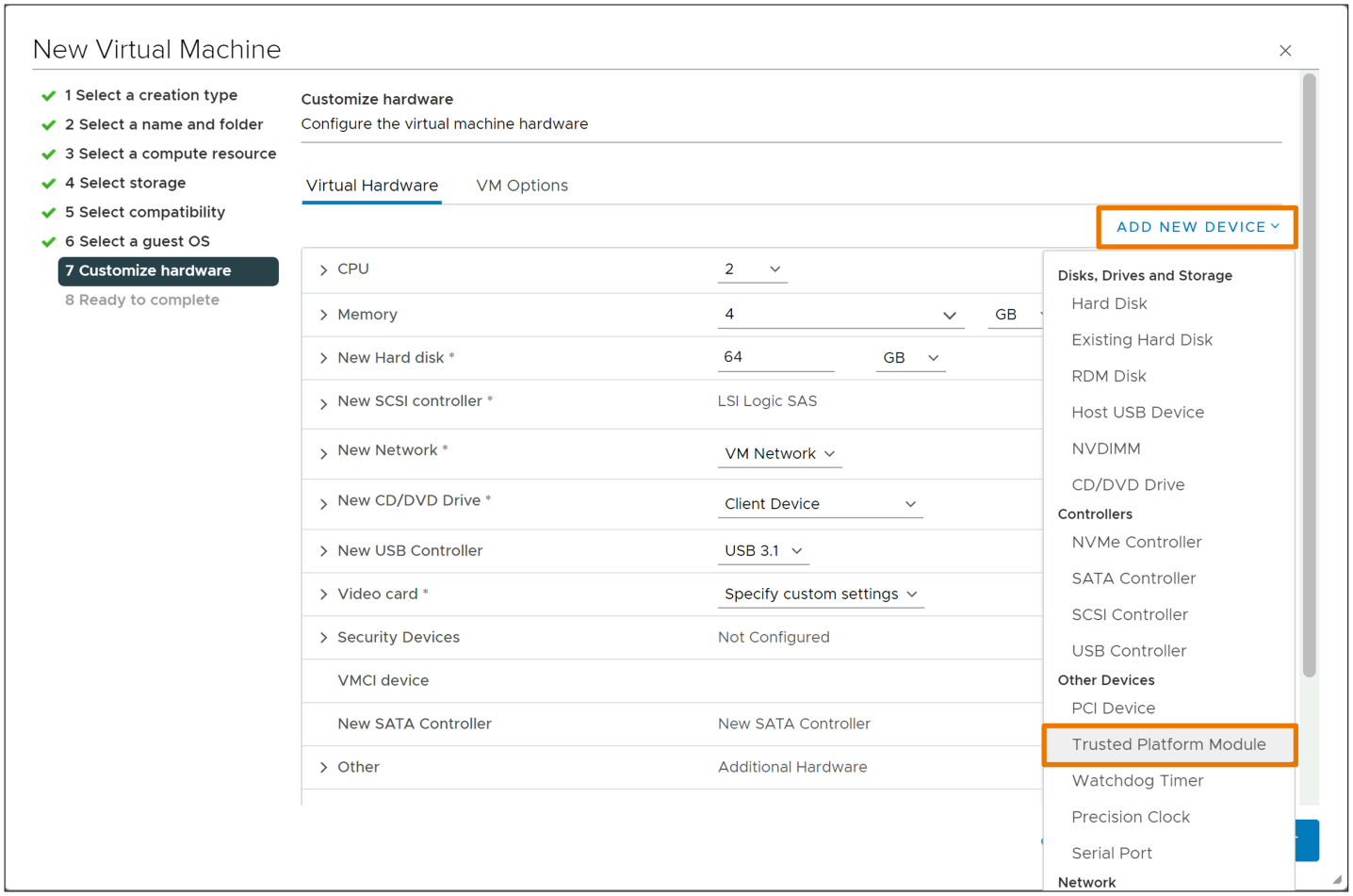
Installing Windows 11 in a Virtual Machine on vSphere 7

Installing Windows 11 in a virtual machine on vSphere 7 requires slightly more manual configuration compared to the vSphere 8.

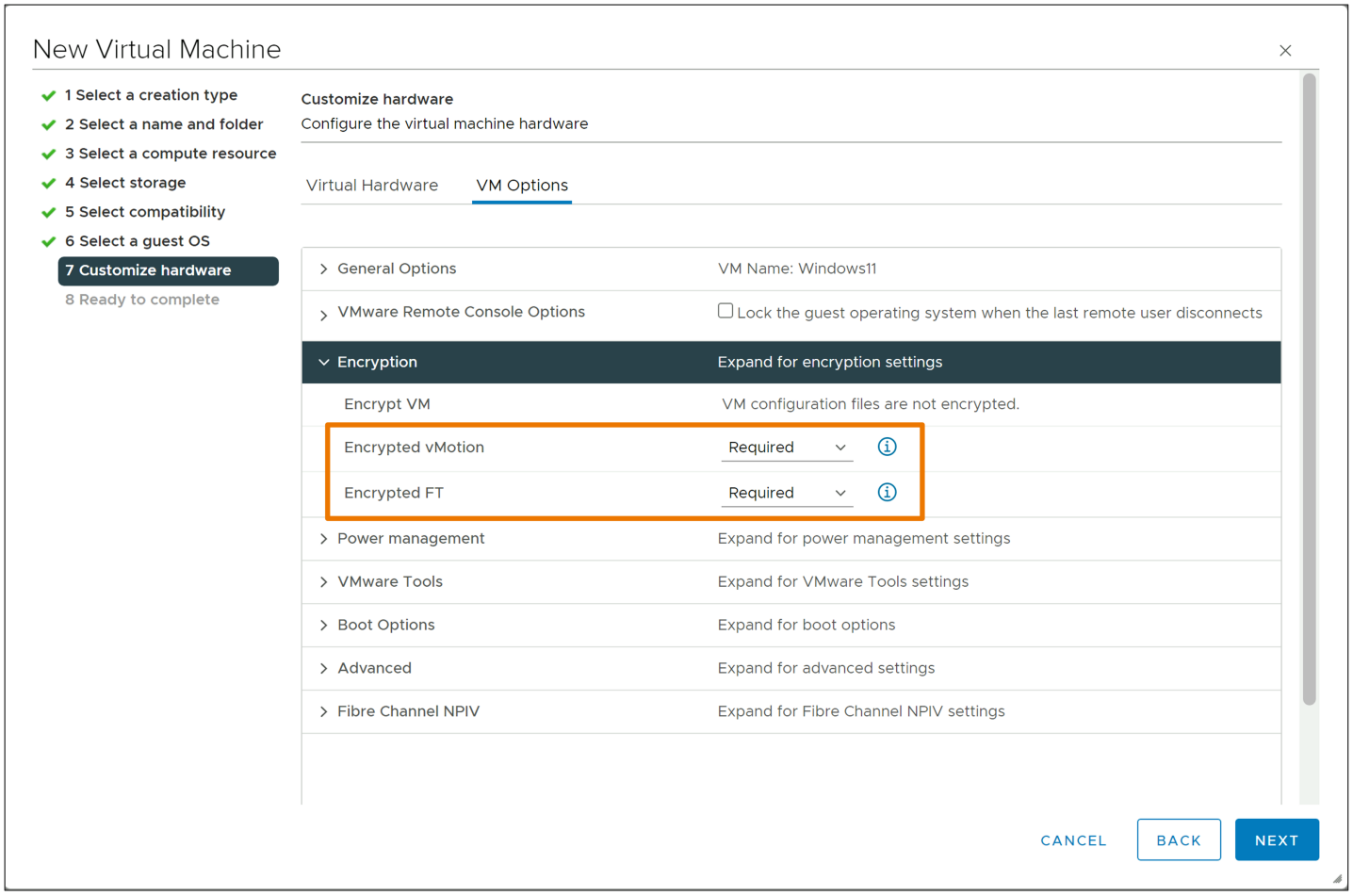
When creating a new virtual machine, using the vSphere Client, select a minimum of virtual machine compatibility with ESXi 6.7 U2 and later (hardware version 15) and choose Microsoft Windows 10 (64-bit) as the Guest OS Version. vSphere 6.7 and vSphere 7 do not currently present Microsoft Windows 11 as a specific Guest OS Version. **vSphere 8 and hardware version 20** presents Microsoft Windows 11 (64-bit) as a selectable Guest OS Version.



A Trusted Platform Module device is not a default device and must be added manually during the new VM creation wizard. On the Customize Hardware page, click Add New Device, and select Trusted Platform Module from the list of devices.



Lastly, navigate to the VM Options tab of the Hardware Customization page. Expand Encryption and set both Encrypted vMotion and Encrypted FT settings to Required. Normally this would not be needed and is a known issue. See KB Article 85974 for more details. **When using vSphere 8 and hardware version 20, these settings are automatically selected for Windows 11 virtual machines.**



Complete the new virtual machine wizard as normal and you are ready to install Windows 11.

See the VMware Guest Operating System Customization Matrix and the Windows 11 Guest Operating System installation guide for more details.

Note: The recommended choice for virtual storage controller is VMware Paravirtual SCSI (PVSCSI).
Refer https://kb.vmware.com/s/article/84200 to add the PVSCSI driver to Windows ISO or provide the driver to Windows during installation by following process mentioned in the section "*To install PVSCSI drivers through CD/DVD drive (Recommended)*" of KB https://kb.vmware.com/s/article/1010398.

Windows 11 22H2 version includes VMware pvscsi drivers as part of the default Windows installation media!

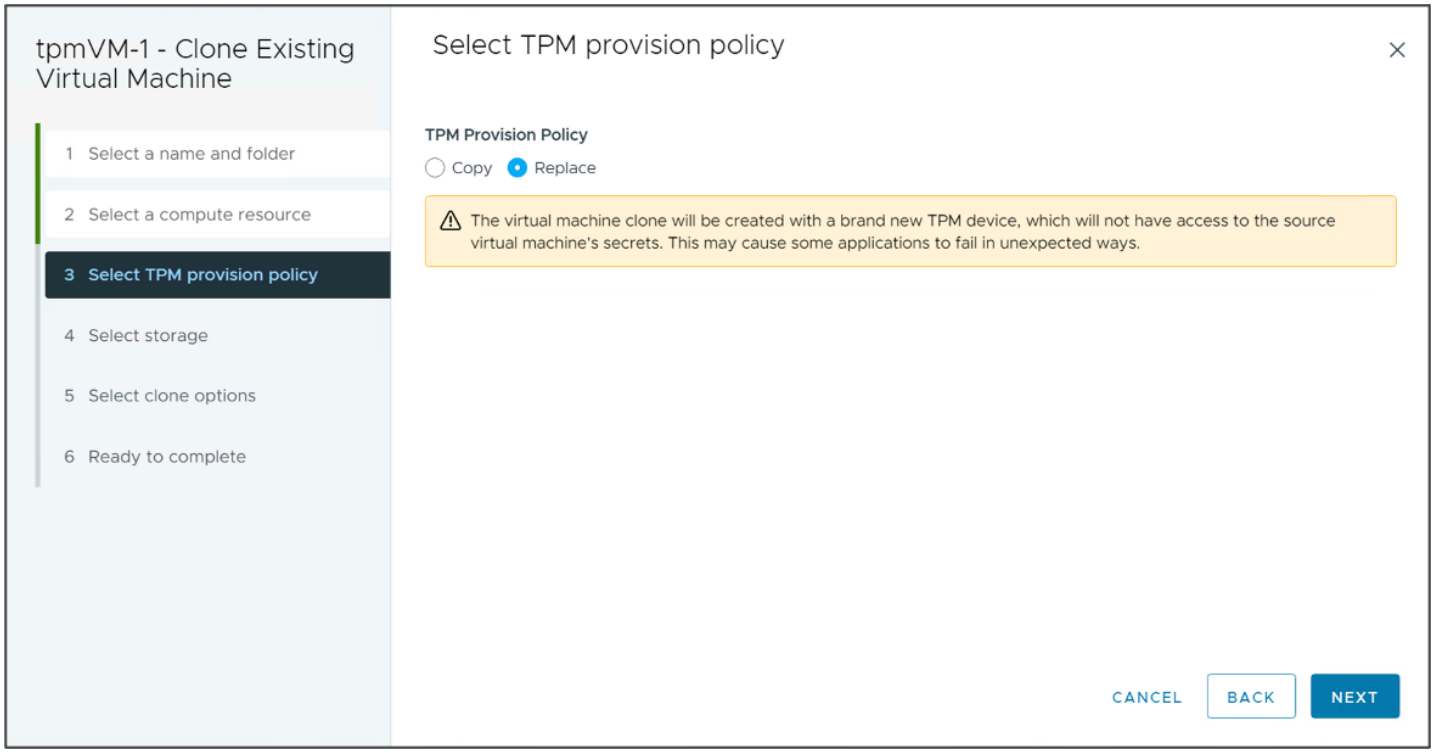
Windows 11 Inbox VMware drivers.

Cloning a virtual machine with a vTPM device

When you clone a virtual machine, that contains a vTPM device, the vTPM device and stored secrets are also cloned. This is desired if Windows features utilizing vTPM, such as Windows BitLocker or Windows Hello, are activated but best practice is to ensure that each Windows 11 virtual machine contains a unique vTPM device.

If you remove or replace the vTPM device on a Windows 11 VM using features like Windows BitLocker or Windows Hello, these features will cease functionality and you may lose access to the Windows operating system or data if you are without the appropriate recovery options.

vSphere 8 introduces the TPM Provision Policy. vTPM devices can be automatically replaced during clone or deployment operations. This allows best practices that each VM contain a unique TPM device be followed and improves vSphere support for Windows 11 deployment at scale. vSphere 8.0 also includes the vpxd.clone.tpmProvisionPolicy advanced setting to make the default clone behaviour for vTPMs to be replaced.



In vSphere 7, you can customize the virtual machine hardware and remove and re-add the vTPM device manually during the clone wizard.

Important: Always be aware of what impact copying or replacing a vTPM device may have on a virtual machine.

- Copy will result in the the clone/deployed virtual machine having access to any stored secrets from the source virtual machine.
- Replace will result in a new vTPM device and the virtual machine will not have access to any secrets from the source virtual machine.

Ensure that you choose the right option for your use-case.

VM Templates with a vTPM device

When you deploy a virtual machine from a VM template containing a vTPM device, the same caveats apply as when cloning a virtual machine with a vTPM device. The vTPM of the deployed VM is an identical copy of that of the template. In vSphere 8, when deploying Windows 11 VMs from template, the TPM Provision Policy is applied and you can either copy or replace the vTPM device during template deployment. In vSphere 7, you can customize the virtual machine hardware and remove and re-add the vTPM device manually during the template deployment wizard.

Virtual machines with a vTPM device can be stored in the VM Template (VMTX) format. Virtual machines with a vTPM device can be stored in a Content Library, but they must be stored as the VM Template (VMTX) format.

For more details on the VM Template format in Content Libraries, see the VMware documentation on, The VM Template as a Content Library Item.

Important: VM Templates with vTPM devices can be deployed from a Content Library. In vSphere 8, currently the default TPM provision policy (copy) is applied and cannot be changed during deployment from a Content Library. The vSphere Client will display a message:

```
Deploy VM template from library workflow does not support changing TPM provision policy.
```

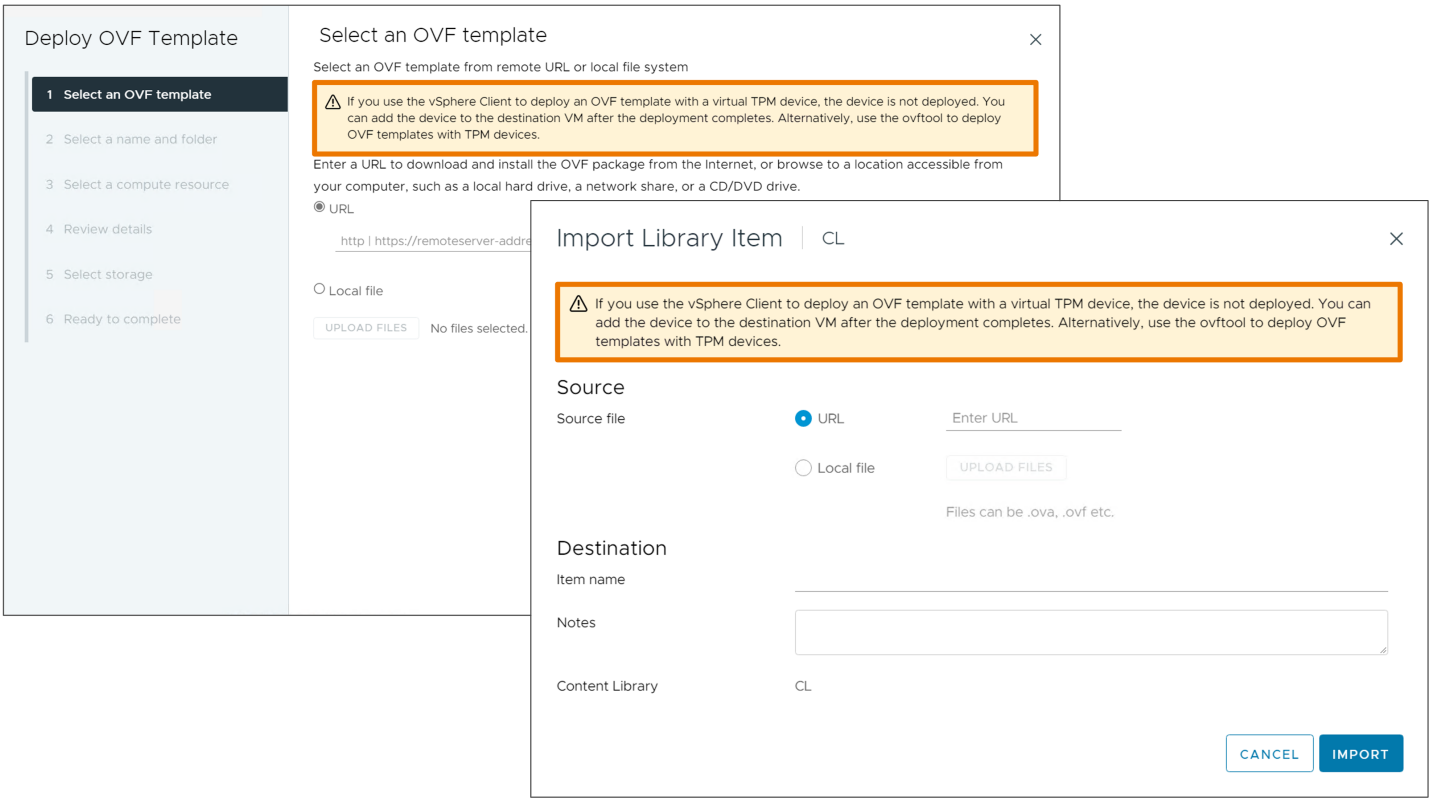
If you wish to use the replace TPM provision policy when deploying from Content Library, change the vCenter advanced

setting *vpxd.clone.tpmProvisionPolicy* to use a value of *replace*.

OVF/OVA Templates with a vTPM device

Virtual machines with a vTPM device do not support the OVF/OVA template format directly. It is not supported to export a virtual machine with a vTPM device to an OVF/OVA file using the vSphere Client. The vTPM device must be first removed before you can export the VM as an OVF/OVA template.

Similarly, when importing an OVF/OVA into vSphere using the vSphere Client, a vTPM device must be manually added to the VM after import. The vSphere Client displays a warning message when deploying an OVF template or importing an OVF to a Content Library stating that the imported VM will not contain a vTPM device, even if the OVF contains a vTPM placeholder. See *Using OVF Tool with vTPM Virtual Machines* below.



Important: The vSphere Client and Content Library service do not currently recognise vTPM placeholder attributes. When importing an OVF/OVA template that does contain vTPM placeholder attributes this section is ignored and the imported virtual machine or template will not have a vTPM device associated with it. You must manually add a vTPM device to the imported machine. VMware is working to improve this workflow in a future release. See *Using OVF Tool with vTPM Virtual Machines* below.

Using OVF Tool with vTPM Virtual Machines

Using the OVF Tool 4.5 and later, vTPM placeholders can be added to virtual machine OVF files during export.

The option **--addDevice:vtpm** can be used to automatically create a vTPM placeholder in the OVF descriptor file during export. You must still first manually remove the vTPM device from the virtual machine before export. The following example command will export the virtual machine named *myvm* and add a vTPM placeholder to the resulting ovf file.

```
ovftool --addDevice:vtpm vi://administrator@vsphere.local:password@vcenter-08.vmw.lab/datacenter/vm/myvm
"C:\export\myvm.ovf"
```

Inspecting the exported OVF file, you should be able to see Virtual TPM placeholder device.

```
<VirtualSystem ovf:id="vm">
  <Info>A virtual machine</Info>
  <Name>vm</Name>
  <OperatingSystemSection ovf:id="1" vmw:osType="windows11_64Guest">
    <Info>The kind of installed guest operating system</Info>
    <Description>Microsoft Windows 11 (64-bit)</Description>
  </OperatingSystemSection>
  <VirtualHardwareSection>
    <Info>Virtual hardware requirements</Info>
    <System>
      <vssd:ElementName>Virtual Hardware Family</vssd:ElementName>
      <vssd:InstanceID>0</vssd:InstanceID>
      <vssd:VirtualSystemIdentifier>vm</vssd:VirtualSystemIdentifier>
      <vssd:VirtualSystemType>vmx-20</vssd:VirtualSystemType>
    </System>
    <Item ovf:required="false">
      <rasd:AutomaticAllocation>false</rasd:AutomaticAllocation>
      <rasd:ElementName>Virtual TPM</rasd:ElementName>
      <rasd:InstanceID>13</rasd:InstanceID>
      <rasd:ResourceSubType>vmware.vtpm</rasd:ResourceSubType>
      <rasd:ResourceType>1</rasd:ResourceType>
    </Item>
```

When using OVF Tool to import a template, that contains a vTPM placeholder, a vTPM device is automatically added to the VM on import. The following example command will import the OVF *myvm.ovf* to the specified datastore and host and automatically add a new vTPM device to the imported virtual machine.

```
ovftool --datastore=esx-ucs-02-local --network="VM Network" "C:\export\myvm.ovf"
vi://administrator@vsphere.local:password@vcenter-08.vmw.lab/datacenter/host/cluster/esx-ucs-02.vmw.lab
```

Important: You do not use the **--addDevice:vtpm** flag when importing an OVF. OVF Tool 4.5 and later automatically recognises the vTPM Placeholder and creates the vTPM device on the imported virtual machine.

See the section **TPM as a Virtual Device in OVF** in the **OVF Tool User Guide 4.5** for more details on using OVF Tool.

Migrating Windows 11 Virtual Machines

vSphere vMotion always uses encryption when migrating encrypted virtual machines. This includes virtual machines configured with vTPM devices. vSphere vMotion supports migrating encrypted virtual machines across vCenter Server instances. To support migrations between vCenter Server instances, each instance must be configured with the same Key Provider.

See the section titled *Minimum Requirements for Migrating or Cloning Encrypted Virtual Machines Across vCenter Server Instances* in Encrypted vSphere vMotion for more details.

When using a vSphere Native Key Provider, to support migrations between vCenter Server instances, you must backup the vSphere Native Key Provider Key Derivation Key (KDK) from one of the vCenter Server instances and restore the same KDK into all other vCenter Server instances.

- Back up a vSphere Native Key Provider
- Restore a vSphere Native Key Provider

Building a Windows 11 Template using a Windows Preinstallation Environment (WinPE) Image

Virtual machines with a vTPM device do not support the OVF/OVA template format. You can use a Windows Preinstallation Environment (WinPE) Image to build a Windows 11 VM without a vTPM device and save that VM as an OVF/OVA template. You can deploy Windows 11 at scale from the template, then add a new unique virtual TPM device into each deployed VM instance. Using a bootable WinPE image provides a simple process to deploy Windows 11 into a VM without a vTPM from the start that is fully supported by Microsoft and VMware.

For detailed steps on how to build a Windows 11 VM using a WinPE image, see the KB Article, Deploy Windows 11 in virtual machine using bootable Windows PE (WinPE) Image (88320).

Learn More

VMware Horizon and Horizon Cloud readiness for Microsoft Windows 11

[KB] VMware Horizon and Horizon Cloud readiness for Microsoft Windows 11

Known Issues

- Windows 11 guest operating system option is not available during virtual machine creation (85665)
- Failed to create a new Virtual Machine with virtual Trusted Platform Module (vTPM) device (85974)
- Backing up a Native Key Provider fails when accessing via IP (84068)

Replacing a vTPM Device in vSphere

You can remove and re-add a vTPM device. Doing so causes you to lose all created keys associated with the vTPM, and data protected by those keys. Make sure that you have a backup and recovery method for any data that is protected or encrypted by the vTPM. This is equivalent to replacing a physical TPM device with new hardware.

- Remove Virtual Trusted Platform Module from a Virtual Machine
- Enable Virtual Trusted Platform Module for an Existing Virtual Machine

Resetting a TPM device in Windows 11

You can clear the keys associated with a TPM device from within Windows 11. Clearing the TPM causes you to lose all created keys associated with the TPM, and data protected by those keys, such as a virtual smart card or a sign in PIN. This retains the existing vTPM device on the virtual machine. Make sure that you have a backup and recovery method for any data that is protected or encrypted by the TPM.

For details, see the Microsoft article
https://docs.microsoft.com/en-us/windows/security/information-protection/tpm/initialize-and-configure-ownership-of-the-tpm .