vSphere Virtual TPM (vTPM) Questions & Answers

Table of contents

vSphere Virtual TPM (vTPM) Questions & Answers 5

Questions & Answers 5

- What is a TPM? 5
- What is a vTPM? 5
- What do I need in order to use a vTPM? 5
- Can I use vTPM on a VM on a standalone ESXi host? 5
- What is an endorsement key? 5
- What is a storage root key? 5
- My hosts do not have physical TPM 2.0 devices. Can I still use virtual TPM (vTPM)? 5
- Is vTPM host hardware-dependent, or can it be implemented on any VMware virtualization platform? 5
- Does the vTPM store data in a physical TPM? 6
- Is a virtual TPM connected/mapped to a hardware TPM? 6
- Is the vTPM a “passthrough” TPM? 6
- Do I need hardware TPMs to use vTPM? 6
- Does the functionality of vTPM depend on the version of vSphere? 6
- Are there known impacts on vTPM when updating or upgrading vSphere? 6
- I don’t have the option to add a Trusted Platform Module in my VM settings. What’s wrong? 6
- What is the maximum number of virtual machines that can have vTPMs? 6
- Can I add a vTPM to a virtual machine that is powered on? 6
- If I remove a vTPM does the VM become unencrypted? 6
- Can I use a vTPM on a Linux guest operating system? 6
- How do I upgrade to a newer version of vTPM when I upgrade vSphere? 6
- When I create a new VM, should I check the "Encrypt this virtual machine" option? 7
- When I create a new VM and add a vTPM it gives me an error. What should I do? 7
- Can I perform vMotion on a VM with a vTPM? 7
- Where is the vTPM data stored? 7
- What are Virtual Machine (VM) home files? 7
- Do I need a key provider to use vTPM? 7
- Can I rekey a vTPM? 7
- What are the vSphere license levels that support vTPMs? 7
- Do other encryption functions, such as vSAN data-at-rest encryption and full VM Encryption, have specific license level requirements? 7
- Does VMware Cloud on AWS support vTPM? 7
- Does the Google Cloud VMware Engine support vTPM? 7
- Is a vTPM equivalent to a "TPM 2.0?" 7

My organization requires hardware TPMs. Is a vTPM considered a hardware device? 8

How many VMs with vTPMs can I have on one physical ESXi host? 8

Is a vTPM required for Windows 11? 8

Are the virtual machine VMDKs encrypted? 8

Can I use vTPM without encrypting the VM disks? 8

What is the impact of adding a vTPM on a VM's performance? 8

Does a vTPM slow my workload down? 8

How fast is a vTPM? 8

Can I clone a VM with a vTPM? 8

Isn’t cloning a vTPM a bad idea? 8

What is the configuration parameter to control the default behavior of vTPM cloning? 8

Do VMware Workspace ONE and VMware Horizon products support vTPM? 8

Is the vTPM supported by provisioning tools like the Microsoft Deployment Toolkit? 9

Can I replace the vTPM on a VM during a cloning operation? 9

Can I store a VM with a vTPM as a template? 9

Can I export an OVF/OVA of a VM with a vTPM? 9

Can I import an OVF/OVA with a vTPM? 9

Do I need to do anything to configure the vTPM for use by a guest operating system? 9

What are the default vTPM certificates and how do they get installed? 9

Can I replace the certificates in the vTPM? 9

How do I configure the vTPM on the virtual machine? 9

Does vTPM work with vSAN Encryption? 9

Doesn’t the vTPM on an encrypted vSAN datastore double-encrypt the VM? 9

Does the vTPM support Microsoft Bitlocker? 9

Does the vTPM support Microsoft Device Guard? 9

Does the vTPM support Microsoft Credential Guard? 10

Does the vTPM meet DISA STIG requirements for Windows and Windows Server? 10

Do I need a vTPM to use Microsoft Device Guard, Credential Guard, and/or BitLocker? 10

Does vTPM work with vGPUs? 10

Does the vTPM work with wolfTPM? 10

Can a VM with a vTPM be backed up? 10

When I added a vTPM the VM now says “Encrypted” but it is not using an encrypted storage policy. Is that normal? 10

When I added a vTPM I noticed the VM now requires vMotion and Fault Tolerance encryption. Is that normal? 10

Disclaimer 11

Additional Resources 12

Feedback 13

vSphere Virtual TPM (vTPM) Questions & Answers

Questions & Answers

What is a TPM?

A Trusted Platform Module (TPM) is a specialized chip on an endpoint device that stores RSA encryption keys specific to the host system for hardware authentication. It is designed to provide basic security-related functions, primarily involving encryption keys. The TPM is used for a variety of tasks such as ensuring the integrity of platform and user security processes, and for secured storage of artifacts used in authentication processes. Overall, it provides a secure environment to generate, use, and store encryption keys, offering a higher level of security than software alone.

What is a vTPM?

A virtual Trusted Platform Module (vTPM) as implemented in VMware vSphere is a virtual version of a physical TPM 2.0 chip, implemented using VM Encryption. It offers the same functionality as a physical TPM but is used within virtual machines (VMs). With vTPM, each VM can have its own unique and isolated TPM to help secure sensitive information and ensure system integrity. It enables VMs to use security enhancements like BitLocker disk encryption, and to authenticate virtual hardware devices, creating a more secure virtual environment.

What do I need in order to use a vTPM?

You need VMware vSphere 6.7 or newer and a key provider, such as Native Key Provider. Both vTPM and Native Key Provider are licensed for use in all vSphere versions.

Use of VM Encryption beyond vTPM may require additional licensing.

Can I use vTPM on a VM on a standalone ESXi host?

vTPM relies on VM Encryption which is enabled when ESXi is managed by vCenter Server, as part of VMware vSphere.

What is an endorsement key?

The TPM 2.0 Endorsement Key (EK) is a unique and permanent RSA or ECC asymmetric key pair that is generated and stored in the vTPM during instantiation. The EK is designed to be non-migratable, which means it cannot be moved to another TPM.

The EK serves two primary purposes: it helps to uniquely identify a TPM (or the device to which it is attached), and it serves as a root of trust for other keys that the TPM generates for use in encryption and digital signing. The EK is typically used indirectly through other keys tied to it, helping ensure that these operations are secure and specific to the TPM and device.

The EK can be used in a privacy-sensitive way by creating an "endorsement key certificate" where the EK is used to sign a statement, which is then signed by a privacy-ca Certificate Authority, thus proving that the statement comes from a legitimate TPM without revealing the EK directly.

What is a storage root key?

The Storage Root Key (SRK) in a TPM 2.0 is a key hierarchy that is created when the TPM is first initialized, or when it's reset. It is derived from a primary seed unique to the TPM and is embedded within the device. This key hierarchy, or tree, is anchored by the SRK.

The SRK is used as a root for storage and management of other keys used by the TPM. The keys managed under the SRK hierarchy are typically wrapped, or encrypted, by the SRK. This means these keys can only be decrypted and used when they are inside the TPM chip itself, providing an additional layer of security.

The SRK essentially enables the TPM to securely generate, store, and handle cryptographic keys, ensuring that these keys can't be used without the TPM, and therefore, providing a root of trust for storage.

My hosts do not have physical TPM 2.0 devices. Can I still use virtual TPM (vTPM)?

Absolutely! vTPMs have nothing to do with a physical TPM, aside from sharing the name “TPM.” The physical TPM is used exclusively by ESXi and is not accessible by VMs. To enable vTPMs, you simply need to configure a key provider in vSphere. Or, on VMware Cloud on AWS, just add a vTPM.

Is vTPM host hardware-dependent, or can it be implemented on any VMware virtualization platform?

A vTPM is not dependent on physical hardware.

Does the vTPM store data in a physical TPM?

No. vTPMs on VMware products do not require or use hardware TPMs.

Is a virtual TPM connected/mapped to a hardware TPM?

No. vTPMs on VMware products do not require or use hardware TPMs for anything.

Is the vTPM a "passthrough" TPM?

No. While other hypervisors use "passthrough" TPMs where they store VM secrets in the host's hardware TPM, VMware does not do that. vTPMs on VMware products do not require or use hardware TPMs.

Do I need hardware TPMs to use vTPM?

No, you do not need hardware TPMs to use vTPM. Although hardware TPMs are inexpensive and significantly improve the security of ESXi, they are strongly recommended but not required for vTPM usage.

Does the functionality of vTPM depend on the version of vSphere?

You need vSphere 6.7 or newer for vTPM, and vSphere 7 Update 2 or newer to use Native Key Provider.

Are there known impacts on vTPM when updating or upgrading vSphere?

Not at this time. Please check the upgrade compatibility matrix for future releases prior to upgrading.

I don't have the option to add a Trusted Platform Module in my VM settings. What's wrong?

A variety of things might need to be checked:

- Have you configured a key provider?
- Have you set a default key provider?
- If you are using Native Key Provider, have you backed up the key provider?
- If you are using Native Key Provider, have you chosen the "Use key provider only with TPM protected ESXi hosts" option? If you did this Native Key Provider will only push support to the hosts with a hardware TPM. If your hosts do not have a hardware TPM then they cannot participate, and you will have issues. Ensure you have the backup file for the Native Key Provider instance, delete the instance, and restore it from the backup but do not check that box this time (yes, it says recommended, but that is only if you have the required hardware). You'll see "TPM2 Device is Required" in the system logs when this happens.
- Is the guest OS set to an option that supports vTPM? When in doubt, try setting the VM to be Windows Server 2019 to see if Trusted Platform Module appears as an option.

To troubleshoot the absence of a Trusted Platform Module option in your VM settings, ensure proper key provider configuration, compatibility with guest OS, and avoid restricting Native Key Provider to TPM-protected ESXi hosts if lacking required hardware.

What is the maximum number of virtual machines that can have vTPMs?

vTPMs are supported on the maximum number of virtual machines possible on vSphere. Please check https://configmax.vmware.com for those configuration limits.

Can I add a vTPM to a virtual machine that is powered on?

No. TPMs are not hot-pluggable hardware components in the physical world, so you cannot do that in the virtual world, either.

If I remove a vTPM does the VM become unencrypted?

If a VM is not otherwise using VM Encryption, such as for its VMDK files, removing the vTPM will cause the VM to no longer be encrypted.

Can I use a vTPM on a Linux guest operating system?

Yes. The device option appears for a selection of Linux distributions. If your distribution does not have direct support, simply set your VM to a supported guest OS, add the vTPM, and set it back. vSphere will not remove the device if it is there. To interact with TPM on a Linux system, you can use various tools and libraries, such as tpm2-tools, tpm2-abrmd, and more.

How do I upgrade to a newer version of vTPM when I upgrade vSphere?

The vTPM is a TPM 2.0 compatible component. If there are virtual hardware changes they will be part of the virtual machine hardware compatibility upgrade process.

When I create a new VM, should I check the "Encrypt this virtual machine" option?

No – selecting this option will encrypt the whole VM. To add a vTPM, simply add the "Trusted Platform Module" virtual device to the VM. vSphere will take care of the rest.

When I create a new VM and add a vTPM it gives me an error. What should I do?

Some versions of vSphere had an order-of-operations issue with the encryption and configuration. Try creating the VM without the vTPM, then, once it is provisioned, add the vTPM.

Can I perform vMotion on a VM with a vTPM?

Yes. VMware vMotion and Storage vMotion work seamlessly.

Because the VM is encrypted, cross-vCenter vMotion will only work if the destination has access to the same key provider as the source. The Native Key Provider can help with that, either as the solution or as a “bridge” between the source and destination if they do not share a Key Management System (KMS). To perform cross-vCenter vMotion with VMware Cloud on AWS, please contact support, as the Native Key Provider instance is not directly configurable.

Where is the vTPM data stored?

vTPM data is stored in the VM configuration, also known as the "home" files, specifically the NVRAM file. The vTPM data is encrypted by VM Encryption.

What are Virtual Machine (VM) home files?

Configuration files associated with the virtual machine that contain VM data and metadata, but are not the VMDK (Virtual Machine Disk) virtual disk files.

For instance, vTPM data is stored in the NVRAM file, which is present in the virtual machine's home directory. The NVRAM file is one of the "home" files.

Do I need a key provider to use vTPM?

Yes. vTPMs use VM Encryption “under the hood” to protect workload secrets. On-premises software like VMware vSphere and VMware Cloud Foundation need the key provider configured before a vTPM can be added.

VMware Cloud on Amazon Web Services (AWS) version 1.19 and newer automatically provision, configure, and protect vSphere Native Key Provider, so you do not have to do anything except add vTPMs to your workloads.

Can I rekey a vTPM?

No, a TPM or vTPM cannot be rekeyed. The Endorsement Key is permanent and the whole TPM would need to be replaced to change it.

What are the vSphere license levels that support vTPMs?

All editions of vSphere 7 and newer are licensed to use vTPM and the Native Key Provider.

Do other encryption functions, such as vSAN data-at-rest encryption and full VM Encryption, have specific license level requirements?

Yes, other encryption functions, such as vSAN data-at-rest encryption and full VM Encryption, are available at specific license levels.

Does VMware Cloud on AWS support vTPM?

Yes. On VMware Cloud on AWS version 1.20 and newer, you can simply add vTPM devices to your workloads.

Does the Google Cloud VMware Engine support vTPM?

Yes. More information can be found on the VMware Cloud Tech Zone.

Is a vTPM equivalent to a "TPM 2.0?"

Yes, the Virtual Trusted Platform Module (vTPM) implements the TPM 2.0 specification and provides the same cryptographic coprocessor, attestation, and secure enclave services that a hardware TPM 2.0 supplies.

My organization requires hardware TPMs. Is a vTPM considered a hardware device?

No, vTPMs are not backed by hardware, but they function identically to a “real” hardware TPM 2.0 device. Everything a workload can do with physical TPM hardware is possible with the vTPM as well.

How many VMs with vTPMs can I have on one physical ESXi host?

You can have as many VMs with virtual Trusted Platform Modules (vTPMs) as you like on one physical ESXi host. The vTPM has no direct limitations related to the physical host.

Is a vTPM required for Windows 11?

Microsoft has included TPM support as a requirement for Windows 11. While there are ways to circumvent these requirements for testing, the vTPM functionality allows you to remain fully supported by Microsoft.

Are the virtual machine VMDKs encrypted?

Enabling a Virtual Trusted Platform Module (vTPM) does not automatically encrypt the VMDK files. If you wish to encrypt them, you need to perform this as a separate action.

Can I use vTPM without encrypting the VM disks?

Yes, you are not required to encrypt the VM disks in order to add a vTPM.

What is the impact of adding a vTPM on a VM's performance?

A vTPM is a low I/O device, so it has minimal impact on performance. However, there may be a slight increase in boot times due to the additional security measures being implemented. If a VM is encrypted, its swap files will also be encrypted. This may cause additional CPU overhead if the VM's memory is being paged to disk by ESXi due to resource overcommitment.

Does a vTPM slow my workload down?

A vTPM is such a low I/O device that, practically speaking, you won’t notice any performance difference. Guest OSes rarely access the TPM. Boot times may increase very slightly.

When you encrypt a VM the swap files will also be encrypted, too. As such, there may be additional CPU overhead if your VM’s memory is being paged to disk by ESXi due to resource overcommitment.

How fast is a vTPM?

Hardware-based TPMs are accessed over a slow serial bus, similar to a modem. A virtual TPM (vTPM), because it is emulated, is much faster than that.

Guest operating systems (OSes) don’t store very much data in a TPM (only kilobytes in total), and don’t read from it very much, so speed is not likely to be a concern.

Can I clone a VM with a vTPM?

On VMware vSphere 6.7 and 7, cloning a virtual machines makes an exact replica of the virtual machine and vTPM. VMware vSphere 8 introduces choices about what to do with the vTPM, so that different use cases can be handled well. It offers to either copy or replace the TPM. 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 functioning, and you may lose access to the Windows operating system or data if you are without the appropriate recovery options.

Isn’t cloning a vTPM a bad idea?

There are many use cases for an exact copy of the original VM, including recovery from application upgrades, testing, backups, snapshot avoidance, and other forms of resilience. An exact copy of a VM has always been what is delivered with cloning. Changing that behavior outright would impact many organizations' workflows, hence why VMware vSphere 8 offers a choice.

What is the configuration parameter to control the default behavior of vTPM cloning?

The vCenter Server parameter vpxd.clone.tpmProvisionPolicy can be set to "copy" or "replace" to control the default behavior when cloning virtual machines with vTPMs.

Do VMware Workspace ONE and VMware Horizon products support vTPM?

Yes. Please check the product documentation for information on how to configure VM templates to deploy unique vTPMs.

Is the vTPM supported by provisioning tools like the Microsoft Deployment Toolkit?

Yes. A vTPM is functionally identical to a hardware TPM. Tools that interact with TPMs will work correctly on virtual machines.

Can I replace the vTPM on a VM during a cloning operation?

VMware vSphere 8 introduces the TPM Provisioning Policy, where vTPM devices can be automatically replaced during clone or deployment operations.

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

Can I store a VM with a vTPM as a template?

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.

Can I export an OVF/OVA of a VM with a vTPM?

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. The OVF Tool can automate the process by adding a vTPM placeholder attribute. See the section “TPM as a Virtual Device in OVF” in the OVF Tool User Guide for more details on using OVF Tool.

Can I import an OVF/OVA with a vTPM?

When importing an OVF/OVA into vSphere using the vSphere Client, a vTPM device must be manually added to the VM after import. The OVF Tool can automate the process by parsing a vTPM placeholder attribute. See the section “TPM as a Virtual Device in OVF” in the OVF Tool User Guide for more details on using OVF Tool.

Do I need to do anything to configure the vTPM for use by a guest operating system?

No. The default vTPM will contain certificates that are compatible with supported guest operating systems.

What are the default vTPM certificates and how do they get installed?

The certificates and keypairs that are populated into the vTPM by default are provided by the VMware Certificate Authority, a component of vCenter Server that manages the certificates for a vSphere cluster. This is a one-time event, done at vTPM instantiation, and includes the endorsement key which serves as the root of the unique identity for the TPM. The VMware Certificate Authority does not store or persist the certificates or keys in any way.

Can I replace the certificates in the vTPM?

Yes. You can replace the certificates in the vTPM using the vSphere APIs or the vSphere Client UI. Most use cases do not require any configuration or alteration of these default certificates, as guest OSes have been tested to work well with them.

How do I configure the vTPM on the virtual machine?

The vTPM can be configured using the virtual BIOS interfaces inside the VM, just as you might do with physical hardware. It is rare that you would need to configure anything to use the vTPM, though.

Does vTPM work with vSAN Encryption?

Yes.

Doesn’t the vTPM on an encrypted vSAN datastore double-encrypt the VM?

Yes, but just a little bit. The vTPM causes the VM configuration files to be encrypted, as well as the swap files. If your virtual machine is paging memory to disk (swapping), this may be an additional concern.

Does the vTPM support Microsoft Bitlocker?

Yes. Environments that use VMware vSAN data-at-rest encryption, like VMware Cloud on AWS SDDC, should be mindful of performance impacts from the additional in-guest encryption, and operational impacts like the ability to store recovery keys for volumes protected by BitLocker.

Does the vTPM support Microsoft Device Guard?

Yes. Microsoft Device Guard builds on Virtualization-Based Security and requires additional VM configuration and guest OS configuration to enable and use.

Does the vTPM support Microsoft Credential Guard?

Yes. Microsoft Credential Guard builds on Virtualization-Based Security and requires additional VM configuration and guest OS configuration to enable and use.

Does the vTPM meet DISA STIG requirements for Windows and Windows Server?

Yes.

Do I need a vTPM to use Microsoft Device Guard, Credential Guard, and/or BitLocker?

Not necessarily. Many compliance frameworks require a TPM when these features are enabled, but the features themselves may not specifically require a TPM. Check the documentation for the guest OS.

Does vTPM work with vGPUs?

Yes. However, vGPUs and DirectPath I/O do not work with Virtualization-Based Security, due to the multiple layers of hypervisors in use when Microsoft Credential Guard is enabled in the guest. This is a limitation in CPU hardware, not a limitation in vSphere or VMware Cloud on AWS.

Does the vTPM work with wolfTPM?

According to the vendor, wolfTPM is tested against the TPM 2.0 specification, which is what vTPM implements.

Can a VM with a vTPM be backed up?

Yes. Please consult your backup vendor for more information about their support for virtual TPM and encrypted VMs.

When I added a vTPM the VM now says “Encrypted” but it is not using an encrypted storage policy. Is that normal?

Yes, it is correct. The process of adding a vTPM handles the VM home file encryption but does not change the storage policy itself.

When I added a vTPM I noticed the VM now requires vMotion and Fault Tolerance encryption. Is that normal?

Correct. VMs using VM Encryption (which is what powers vTPM “under the hood”) are always required to be protected when vMotioned.

VMware recommends configuring these settings to “Required” on all virtual machines and workloads. For more information about recommended security settings, please see the vSphere Security Configuration Guide.

Disclaimer

This document is intended to provide general guidance for organizations that are considering VMware solutions. The information contained in this document is for educational and informational purposes only. This document is not intended to provide advice and is provided "AS IS." VMware makes no claims, promises, or guarantees about the accuracy, completeness, or adequacy of the information contained herein. Organizations should engage appropriate legal, business, technical, and audit expertise within their specific organization for review of requirements and effectiveness of implementations.

Additional Resources

Please visit the vSphere security resources at https://core.vmware.com/security.

Feedback

The purpose of this document is to answer questions that may fall outside the scope of product documentation and system design guidance. Your feedback is valuable. To comment on this document please use the feedback mechanisms on this page. Thank you.