

# Image Version Encryption\_ACG

Last updated by | Kevin Gregoire | Feb 7, 2023 at 9:16 AM PST

## Tags

cw.ACG

cw.Azure-Encryption

cw.TSG

cw.Reviewed-12-2022

## Contents

- [Summary](#)
- [Prerequisites](#)
- [Steps](#)
- [Limitations](#)
- [Creating VM from Encrypted Image version](#)
- [Public Documents](#)

## Summary

Shared Image Gallery image versions were encrypted at rest with platform-managed keys, until now.



Now, the image versions can be encrypted through the below options:

- o PMK- Platform Managed Keys
- o CMK- Customer Managed Keys
- o Dual encryption: PMK+CMK

You also have the option to encrypt Shared Image Gallery image versions at a disk level.

## Prerequisites

You must already have a disk encryption set in each region where you want to replicate your image.

- To use only a customer-managed key, see the articles about enabling customer-managed keys with server-side encryption by using the Azure portal or PowerShell. <https://learn.microsoft.com/en-us/azure/virtual-machines/windows/disks-enable-customer-managed-keys-powershell> 
- To use both platform-managed and customer-managed keys (for double encryption), see the articles about enabling double encryption at rest by using the Azure portal or PowerShell. <https://learn.microsoft.com/en-us/azure/virtual-machines/disks-enable-double-encryption-at-rest-portal> 

## Steps

To create encrypted image version through Portal, you can follow the below steps:

1. On the Create VM image version, select the Encryption tab.

## Create VM image version ...

Basics Replication **Encryption** Tags Review + create

Create a new image that can be used to deploy virtual machines and virtual machine scale sets. With a shared image, you can easily replicate the image to Azure regions around the world and manage versions of the image. [Learn more](#)

Looking for managed images? [Click here to create](#)

### Project details

Subscription \* ⓘ

Resource group \* ⓘ

[Create new](#)

2. In the Encryption type, select any one of the below options.

## Create VM image version ...

Basics Replication **Encryption** Tags Review + create

Azure offers server-side encryption with platform-managed keys by default for VM image versions. You may optionally choose to use a customer-managed key with a disk encryption set. [Learn more](#)

SSE encryption type \*

(Default) Encryption at-rest with a platform-managed key

(Default) Encryption at-rest with a platform-managed key

Encryption at-rest with a customer-managed key

Double encryption with platform-managed and customer-managed keys

3. For Customer-managed key and Double encryption with PMK+CMK, you need to select the Disk name and Disk Encryption set.

## Create VM image version ...

Basics Replication **Encryption** Tags Review + create

Azure offers server-side encryption with platform-managed keys by default for VM image versions. You may optionally choose to use a customer-managed key with a disk encryption set. [Learn more](#)

SSE encryption type \*

Double encryption with platform-managed and customer-managed keys

 You must use customer-managed keys for all disks or snapshots based on the encryption type selected.

EAST US

Disk name

Disk Encryption Set

OS disk

Select a disk encryption set

The value must not be empty.

## Limitations


When you're using customer-managed keys for encrypting images in an Azure Compute Gallery, these limitations apply:

- Encryption key sets must be in the same subscription as your image.
- Encryption key sets are regional resources, so each region requires a different encryption key set.
- You can't copy or share images that use customer-managed keys.
- After you've used your own keys to encrypt a disk or image, you can't go back to using platform-managed keys for encrypting those disks or images.
- This feature does not currently support the Image version Source as VM image version and Storage Blob (VHDs).

## Create VM image version ...

Basics Replication **Encryption** Tags Review + create

Azure offers server-side encryption with platform-managed keys by default for VM image versions. You may optionally choose to use a customer-managed key with a disk encryption set. [Learn more](#)

 VM image version source does not currently support customer-managed key encryption. You must choose a different Source on the Basics tab to enable customer-managed key encryption.


## Creating VM from Encrypted Image version

You can create a VM from an image version and use customer-managed keys to encrypt the disks. When you create the VM in the portal, on the Disks tab, select Encryption at-rest with customer-managed keys or Double

encryption with platform-managed and customer-managed keys for Encryption type. You can then select the encryption set from the drop-down list.

## Public Documents

<https://learn.microsoft.com/en-us/azure/virtual-machines/image-version-encryption> 

<https://learn.microsoft.com/en-us/azure/virtual-machines/windows/disks-enable-customer-managed-keys-powershell> 

<https://learn.microsoft.com/en-us/azure/virtual-machines/disks-enable-double-encryption-at-rest-portal> 