
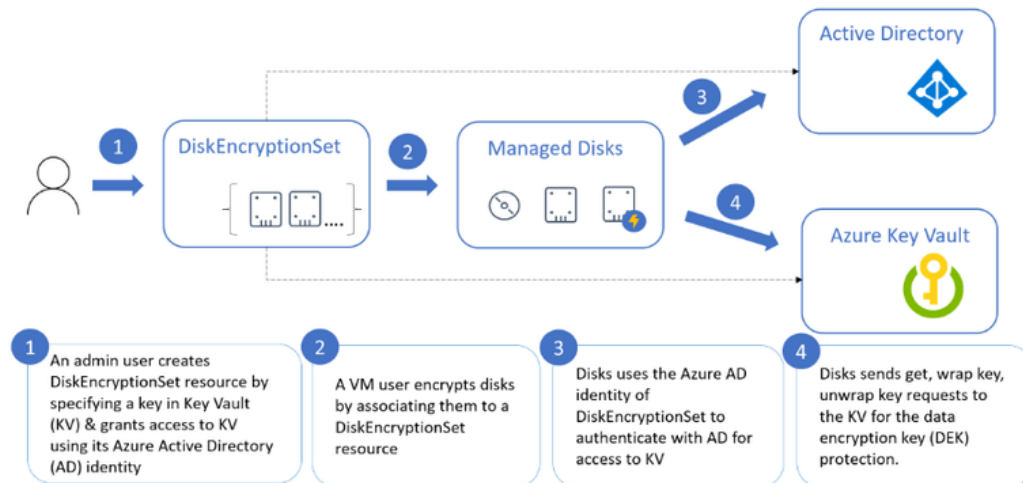


# Encrypting Disks with Disk Encryption Sets

Detailed Process:

 [Azure portal](#) - [Enable customer-managed keys with SSE - managed disks - Azure Virtual Machines](#)

## SSE+CMK Workflow



The following list explains the diagram in more detail:

1. An Azure Key Vault administrator creates key vault resources.
2. The key vault admin either imports their RSA keys to Key Vault or generate new RSA keys in Key Vault.
3. That administrator creates an instance of Disk Encryption Set resource, specifying an Azure Key Vault ID and a key URL. Disk Encryption Set is a new resource introduced for simplifying the key management for managed disks.
4. When a disk encryption set is created, a [system-assigned managed identity](#) is created in Microsoft Entra ID and associated with the disk encryption set.
5. The Azure key vault administrator then grants the managed identity permission to perform operations in the key vault.
6. A VM user creates disks by associating them with the disk encryption set. The VM user can also enable server-side encryption with customer-managed keys for existing resources by associating them with the disk encryption set.
7. Managed disks use the managed identity to send requests to the Azure Key Vault.
8. For reading or writing data, managed disks sends requests to Azure Key Vault to encrypt (wrap) and decrypt (unwrap) the data encryption key in order to perform encryption and decryption of the data.

To revoke access to customer-managed keys, see [Azure Key Vault PowerShell](#) and [Azure Key Vault CLI](#). Revoking access effectively blocks access to all data in the storage account, as the encryption key is inaccessible by Azure Storage.