

Managed Disk Storage Service Encryption with CMK_Encryption

Last updated by | Kevin Gregoire | Mar 29, 2022 at 11:47 AM PDT

Tags

cw.Azure-Encryption

cw.How-To

Contents

- [Overview](#)
 - [Supported Regions](#)
 - [Limitations](#)
- [Soft Delete and Purge Protection for Key Vault](#)
 - [Enable Soft Delete and Purge Protection on a Azure Key Va...](#)
 - [PowerShell](#)
 - [CLI](#)
 - [Verify if Soft Delete and Purge Protection is enabled on a ...](#)
 - [PowerShell](#)
 - [CLI](#)
- [How to create a VM with disk encrypted using SSE with CMK](#)
- [Training](#)
- [Need additional help or have feedback?](#)

Overview

Today, Azure Managed Disks are encrypted with Microsoft managed keys by default. Also, [Azure Disk encryption](#) ☑ uses the [BitLocker](#) ☑ feature of Windows and the [DM-Crypt](#) ☑ feature of Linux to encrypt Managed Disks with customer-managed keys (CMK) within the guest VM. This document talks about server-side encryption with CMK for Standard HDD, Standard SSD, and Premium SSD Managed Disks in the private preview. It will give you control of the encryption keys to meet your security and compliance needs in a few clicks. It does not impact the performance of your VMs and works for all the OS types and images as the encryption happens in the Storage service.

It is integrated with [Azure Key Vault](#) ☑ (AKV) that provides highly available and scalable secure storage for RSA cryptographic keys backed by Hardware Security Modules (HSMs). You must enable "Do Not Purge" and "Soft Delete" in your AKV to protect yourself against ransomware scenarios. You can either [import your RSA keys](#) ☑ to AKV or generate new RSA keys in AKV.

You have full control of your keys. Managed Disks uses [system-assigned managed identity](#) ☑ (MI) in your Azure Active Directory for accessing keys in AKV. You can rest assured that an untrusted identity does not use your keys by monitoring the key usage in AKV. Also, a user with required permissions in AKV must first grant permissions to

Managed Disks before it can access the keys. It allows you to prevent Managed Disks from accessing your keys by either disabling your keys or by revoking access controls for your keys. Revoking access to keys will bring your VMs and disks down as Azure Storage cannot read or write to the disks.

Azure Storage handles the encryption and decryption in a fully transparent fashion using [envelope encryption](#). It encrypts data using an [AES](#) 256 based data encryption key (DEK), which is, in turn, protected using the CMK stored in Azure Key Vault. This allows you to rotate (not available in preview) your keys periodically as per your compliance policies without impacting your VMs. When you rotate your keys, Azure Storage re-encrypts the DEKs with the new CMKs. This does not result in re-encryption of the data, and there is no other action required from you.

To enable CMK for Managed Disks, you must first create an instance of a new resource type called as DiskEncryptionSet which represents a CMK. You must associate your disks, snapshots, and images with a DiskEncryptionSet to encrypt them with CMK.

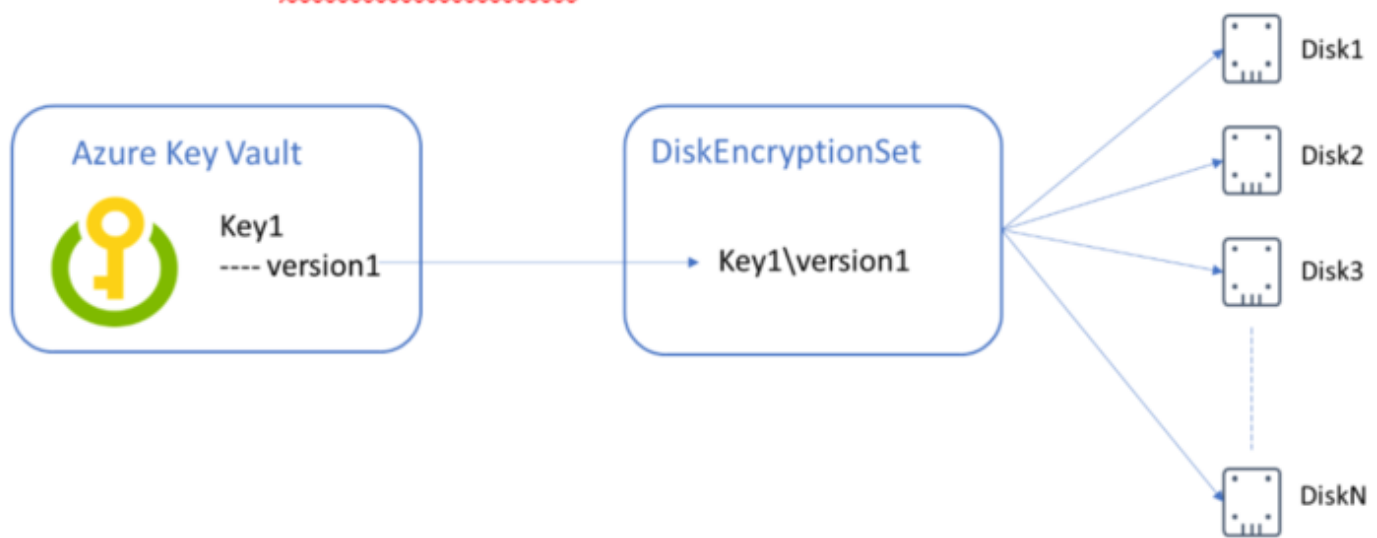


Figure 2: SSE with CMK setup

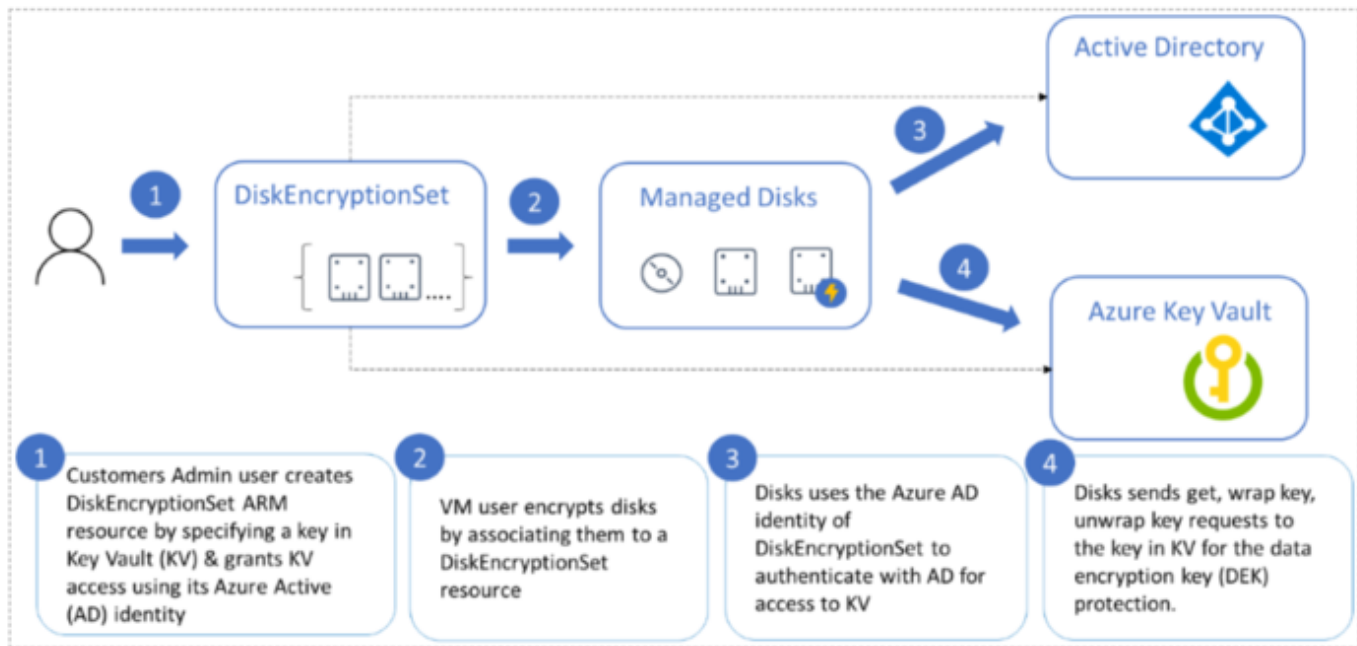


Figure 3 SSE with CMK workflow

Supported Regions

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption#supported-regions>

Limitations

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption#restrictions>

Soft Delete and Purge Protection for Key Vault

Managed Disk Encryption using this CMK feature is only supported with Key Vaults which have [Soft Delete](#) and [Purge Protection](#) features enabled on them.

- Enabling 'soft delete' on a key vault is an irreversible action. Once the soft-delete property has been set to "true", it cannot be changed or removed.
- You can enable purge protection only if soft-delete is also enabled.

Enable Soft Delete and Purge Protection on a Azure Key Vault

[PowerShell](#)

New Key Vault

```
New-AzKeyVault -Name ContosoVault -ResourceGroupName ContosoRG -Location westus -EnableSoftDelete -EnablePurgePr
```

Existing Key Vault

```
($resource = Get-AzResource -ResourceId (Get-AzKeyVault -VaultName "ContosoVault").ResourceId).Properties | Add-
$resource.properties | Add-Member -MemberType NoteProperty -Name enableSoftDelete -Value 'True'

Set-AzResource -resourceid $resource.ResourceId -Properties $resource.Properties
```

CLI

New Key Vault

```
az keyvault create --name ContosoVault --resource-group ContosoRG --location westus --enable-soft-delete true --
```

Existing Key Vault

```
az keyvault update --name ContosoVault --resource-group ContosoRG --enable-soft-delete true --enable-purge-prote
```

Verify if Soft Delete and Purge Protection is enabled on a Azure Key Vault

PowerShell

```
$vault = Get-AzResource -ResourceId /subscriptions/051fef71-2b97-4447-8e56-fb02899520d7/resourceGroups/2304/prov
$vault.properties

sku                : @{family=A; name=standard}
tenantId           : 72f988bf-86f1-41af-91ab-2d7cd011db47
accessPolicies     : {@{tenantId=72f988bf-86f1-41af-91ab-2d7cd011db47; objectId=0a92b54d-2886-48ed-9b5
enabledForDeployment : False
enabledForDiskEncryption : False
enabledForTemplateDeployment : False
enableSoftDelete    : True
enablePurgeProtection : True
vaultUri            : https://ssecmk.vault.azure.net/
provisioningState    : Succeeded
```

CLI

```
az keyvault show --name SSECMK
```

```
{
  "id": "/subscriptions/051fef71-2b97-4447-8e56-fb02899520d7/resourceGroups/2304/providers/Microsoft.KeyVault/vau
  "location": "centraluseuap",
  "name": "SSECMK",
  "properties": {
    "accessPolicies": [
      {
        "applicationId": null,
        "objectId": "0a92b54d-2886-48ed-9b57-921dbf4a6dcf",
        "permissions": {
          "certificates": [
            "Get",
            "List",
            "Update",
            "Create",
            "Import",
            "Delete",
            "Recover",
            "Backup",
            "Restore",
            "ManageContacts",
            "ManageIssuers",
            "GetIssuers",
            "ListIssuers",
            "SetIssuers",
            "DeleteIssuers",
            "Purge"
          ],
          "keys": [
            "Get",
            "List",
            "Update",
            "Create",
            "Import",
            "Delete",
            "Recover",
            "Backup",
            "Restore",
            "Decrypt",
            "Encrypt",
            "UnwrapKey",
            "WrapKey",
            "Verify",
            "Sign",
            "Purge"
          ],
          "secrets": [
            "Get",
            "List",
            "Set",
            "Delete",
            "Recover",
            "Backup",
            "Restore",
            "Purge"
          ],
          "storage": []
        },
        "tenantId": "72f988bf-86f1-41af-91ab-2d7cd011db47"
      },
      {
        "applicationId": null,
        "objectId": "e941d50e-b59a-4784-94fb-b5e015fae3bc",
        "permissions": {
          "certificates": [],
          "keys": [
            "wrapkey",
            "unwrapkey",

```

```

    "get"
  ],
  "secrets": [],
  "storage": []
},
"tenantId": "72f988bf-86f1-41af-91ab-2d7cd011db47"
}
],
"createMode": null,
"enablePurgeProtection": true,
"enableSoftDelete": true,
"enabledForDeployment": false,
"enabledForDiskEncryption": false,
"enabledForTemplateDeployment": false,
"networkAcls": null,
"provisioningState": "Succeeded",
"sku": {
  "name": "standard"
},
"tenantId": "72f988bf-86f1-41af-91ab-2d7cd011db47",
"vaultUri": "https://ssecmk.vault.azure.net/"
},
"resourceGroup": "2304",
"tags": {},
"type": "Microsoft.KeyVault/vaults"
}

```

How to create a VM with disk encrypted using SSE with CMK


[Portal](#) 

[PowerShell](#) 

Training

<https://msit.microsoftstream.com/video/304b0efa-88c1-4f30-8638-3c658b32066b> 

Need additional help or have feedback?

<i>To engage the Azure Encryption SMEs...</i>	<i>To provide feedback on this page...</i>	<i>To provide kudos on this page...</i>
<p>Please reach out to the Azure Encryption SMEs  for faster assistance.</p> <p>Make sure to use the Ava process for faster assistance.</p>	<p>Use the Azure Encryption Feedback form to submit detailed feedback on improvements or new content ideas for Azure Encryption.</p> <p>Please note the link to the page is required when submitting feedback on existing pages! If it is a new content idea, please put N/A in the Wiki Page Link.</p>	<p>Use the Azure Encryption Kudos form to submit kudos on the page. Kudos will help us improve our wiki content overall!</p> <p>Please note the link to the page is required when submitting kudos!</p>