

Encrypt Disk with KEK_Encryption

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

Tags

cw.Azure-Encryption

cw.How-To





Contents

- [Scenario](#)
- [Prerequisites for Single Pass](#)
- [Encrypt the IaaS Virtual Machine with Single Pass \(Powershell\)](#)
- [Encrypt the IaaS Virtual Machine with Single Pass \(CLI\)](#)
- [Encrypt the IaaS Virtual Machine with Single Pass \(Template\)](#)
- [Encrypt the IaaS Virtual Machine \(Portal\)](#)
- [Prerequisites for Dual Pass](#)
- [Encrypt the IaaS Virtual Machine with KEK \(Powershell\)](#)
- [Process to encrypt VM with KEK- Template](#)
- [Get a list of all encrypted VMs in your subscription](#)
- [Get a list of all disk encryption secrets used for encrypting ...](#)
- [Need additional help or have feedback?](#)

Scenario

The customer would like to encrypt the IaaS Virtual Machine with KEK (wrapped BEK) key

Prerequisites for Single Pass

1. Azure subscription: an active, valid Azure Subscription is needed
2. Azure PowerShell: Please use the latest version of Azure PowerShell SDK version to configure Azure Disk Encryption. Download it from [here](#) . Azure Disk Encryption is *NOT* supported by [Azure SDK version 1.1.0](#) . If you are receiving an error related to using Azure PowerShell 1.1.0, please see [this article](#) . Once Powershell is installed, install the Az Module with the command `Install-Module -Name Az -AllowClobber`
3. Azure Key Vault: Azure Disk Encryption securely stores the encryption secrets in a specified Azure Key Vault. Please refer to [Azure Key Vault](#)  for more details on how to setup a Key Vault in Azure. In order to make sure the encryption secrets don't cross regional boundaries, **Azure Disk Encryption needs the Key Vault and the VM to be located in the same region. Please create and use a Key Vault that is in the same region as the VM to be encrypted.**
4. Azure Key Vault Key: In Azure Key Vault, select Keys from the *SETTINGS* column. Select the Key that you want to use. If you don't have a key, then you need to create a key. Select *Generate/Import*, from the new window, you only need to input the *Name*. Then select *Create*. Once created, you will be able to select the

key *NAME*, then select the *CURRENT VERSION*, then copy the *Key Identifier*. This will be the *KeyEncryptionKeyUrl*.

5. IaaS VM in Azure: Azure Disk Encryption works only on IaaS VMs (virtual machines created using the Azure Resource Management model). Please refer to [Different ways to create a Windows virtual machine with Resource Manager](#) for information on how to create IaaS virtual machines in Azure. Please create a VM in the same region as the Key Vault. Latest gallery images in Azure are optimized to finish encryption operation quickly. So it is recommended to create VMs using the latest gallery images.

Encrypt the IaaS Virtual Machine with Single Pass (Powershell)

1. Run the following on an elevated PS session

```
Connect-AzAccount
Get-AzSubscription
Select-AzSubscription -Subscription "<your subscription>"

$KVRGName = 'MyKeyVaultResourceGroup';
$VMRGName = 'MyVirtualMachineResourceGroup';
$vmName = 'MyExtraSecureVM';
$KeyVaultName = 'MySecureVault';
$keyEncryptionKeyName = 'MyKeyEncryptionKey';
$KeyVault = Get-AzKeyVault -VaultName $KeyVaultName -ResourceGroupName $KVRGName;
$diskEncryptionKeyVaultUrl = $KeyVault.VaultUri;
$KeyVaultResourceId = $KeyVault.ResourceId;
$keyEncryptionKeyUrl = (Get-AzKeyVaultKey -VaultName $KeyVaultName -Name $keyEncryptionKeyName).Key.k

Set-AzVMDiskEncryptionExtension -ResourceGroupName $VMRGName -VMName $vmName -DiskEncryptionKeyVaultU
```

2. To verify encryption process use

```
Get-AzVmDiskEncryptionStatus -ResourceGroupName $VMRGName -VMName $vmName
```

Encrypt the IaaS Virtual Machine with Single Pass (CLI)

1. Run the following on an elevated CLI session

```
az vm encryption enable --resource-group "MyVirtualMachineResourceGroup" --name "MySecureVM" --disk-e
```

2. You can verify the status of disks being encrypted with the following command

```
az vm show --name MyVM -g MyResourceGroup
```

3. If you are successful, you should see the following output confirming the VM encryption was successful:

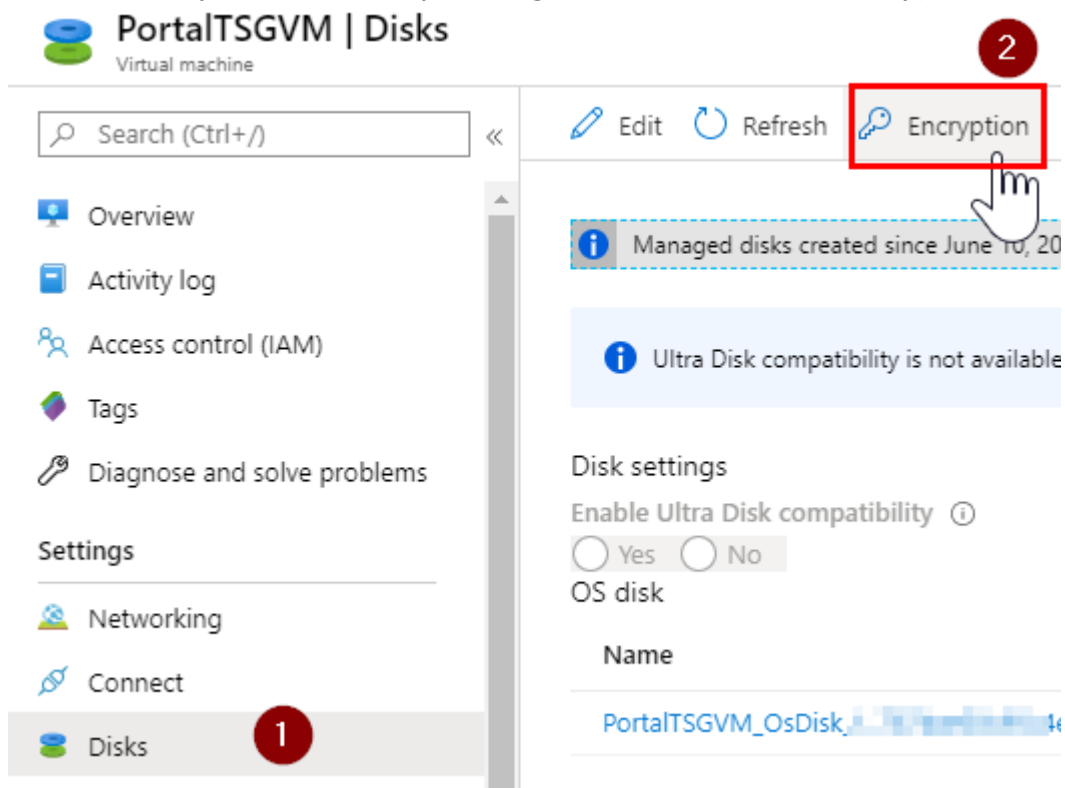
"EncryptionOperation": "EnableEncryption"

Encrypt the IaaS Virtual Machine with Single Pass (Template)


1. Use the template found [here](#) to encrypt the virtual machine.
2. Once you are on the Azure Quickstart Template, fill in the required fields. You can then save the template so that you can reuse when needed. For KEK, fill the KeK Encryption Key URL field.
3. Select the Purchase button to run the template.



Encrypt the IaaS Virtual Machine (Portal)

1. Select the VM you want to encrypt and go to disks. Then select encryption at the top.



2. Select if you want to encrypt only the OS or OS and data from the dropdown menu.

**Encryption**
PortalTSGVM

 Save  Discard

Azure Disk Encryption (ADE) provid

Disks to encrypt ⓘ

None

None

OS disk

OS and data disks

3. Select the encryption settings option for adding a Key Vault

Encryption settings

Azure Disk Encryption is integrated with Azure Key Vault to help manage encryption keys. As a prerequisite, you need to have an existing key vault with encryption permissions set. For additional security, you can create or choose an optional key encryption key to protect the secret.

[Select a key vault and key for encryption](#)

Key vault * ⓘ

None

Key ⓘ

None

Version ⓘ

None

4. Select the Key Vault you plan to use. Add the Key and the Version to encrypt with KEK.

Select key from Azure Key Vault

Key vault *

[Create new](#)

Key

[Create new](#)

Version ⓘ

[Create new](#)

Prerequisites for Dual Pass

1. Azure subscription: an active, valid Azure subscription is needed.
2. Azure PowerShell: Please use the latest version of Azure PowerShell SDK version to configure Azure Disk Encryption. Download it from [here](#) ☐. Azure Disk Encryption is *NOT* supported by [Azure SDK version 1.1.0](#) ☐. If you are receiving an error related to using Azure PowerShell 1.1.0, please see [this article](#) ☐. Once Powershell is installed, install the Az Module with the command `Install-Module -Name Az -AllowClobber`
3. Azure Key Vault: Azure Disk Encryption securely stores the encryption secrets in a specified Azure Key Vault. Please refer to [Azure Key Vault](#) ☐ for more details on how to setup a Key Vault in Azure. In order to make sure the encryption secrets don't cross regional boundaries, **Azure Disk Encryption needs the Key Vault and the VM to be located in the same region. Please create and use a Key Vault that is in the same region as the VM to be encrypted.**
4. Azure Key Vault Key: In Azure Key Vault, select Keys from the *SETTINGS* column. Select the Key that you want to use. If you don't have a key, then you need to create a key. Select *Generate/Import*, from the new window, you only need to input the *Name*. Then select *Create*. Once created, you will be able to select the key *NAME*, then select the *CURRENT VERSION*, then copy the *Key Identifier*. This will be the *KeyEncryptionKeyUrl*.
5. Azure Active Directory Client ID and Secret: In order to write encryption secrets to a specified Key Vault, Azure Disk Encryption needs the Client ID and the Client Secret of the Azure Active Directory application that has permissions to write secrets to the specified Key Vault. Please refer to [Azure Key Vault](#) ☐ for more detail on how to get the Azure Active Directory Client ID and Client Secret using Azure portal.
6. IaaS VM in Azure: Azure Disk Encryption works only on IaaS VMs (virtual machines created using the Azure Resource Management model). Please refer to [Different ways to create a Windows virtual machine with Resource Manager](#) ☐ for information on how to create IaaS virtual machines in Azure. Please create a VM in the same region as the Key Vault. Latest gallery images in Azure are optimized to finish encryption operation quickly. So it is recommended to create VMs using the latest gallery images.

Encrypt the IaaS Virtual Machine with KEK (Powershell)

1. Setup your variables

```
Connect-AzAccount
Get-AzSubscription
Select-AzSubscription -Subscription "<your subscription>"

$RGName = "MyResourceGroup"
$VMName = "MyTestVM"

$AADClientID = "<clientID of your Azure AD app>"
$AADClientSecret = "<clientSecret of your Azure AD app>"

$VaultName= "MyKeyVault"
$KeyVault = Get-AzKeyVault -VaultName $VaultName -ResourceGroupName $RGName
$DiskEncryptionKeyVaultUrl = $KeyVault.VaultUri
$KeyVaultResourceId = $KeyVault.ResourceId
$VolumeType = "All"

$KEKName = "MyKeyEncryptionKey"
$KEK = Add-AzKeyVaultKey -VaultName $VaultName -Name $KEKName -Destination "Software"
$KeyEncryptionKeyUrl = $KEK.Key.kid
```

2. The Azure fabric needs to access encryption secrets in order to boot the encrypted VM. Use the below cmdlet to set Key Vault access policies to allow Azure platform access the encryption secrets placed in the Key Vault.

```
Set-AzKeyVaultAccessPolicy -VaultName $VaultName -ResourceGroupName $RGName -EnabledForDiskEncryption
```

3. This cmdlet uses the variables initialized above. It is recommended to create IaaS VMs using the latest gallery images to quickly enable encryption.

```
Set-AzVMDiskEncryptionExtension -ResourceGroupName $VMRGname -VMName $vmName -AadClientID $aadClientI
```

4. If you are successful, you should see the following output confirming the VM encryption was successful:

```
RequestId IsSuccessStatusCode StatusCode ReasonPhrase
-----
True      OK OK
```

Please refer to the [Set-AzVMDiskEncryptionExtension](#) cmdlet for full list options and details.


5. Once you have enabled and deployed an encrypted VM, the [Get-AzVmDiskEncryptionStatus](#) cmdlet displays encryption status of OS volume, data volumes and the encryption secret Key Vault URLs of OS volume.

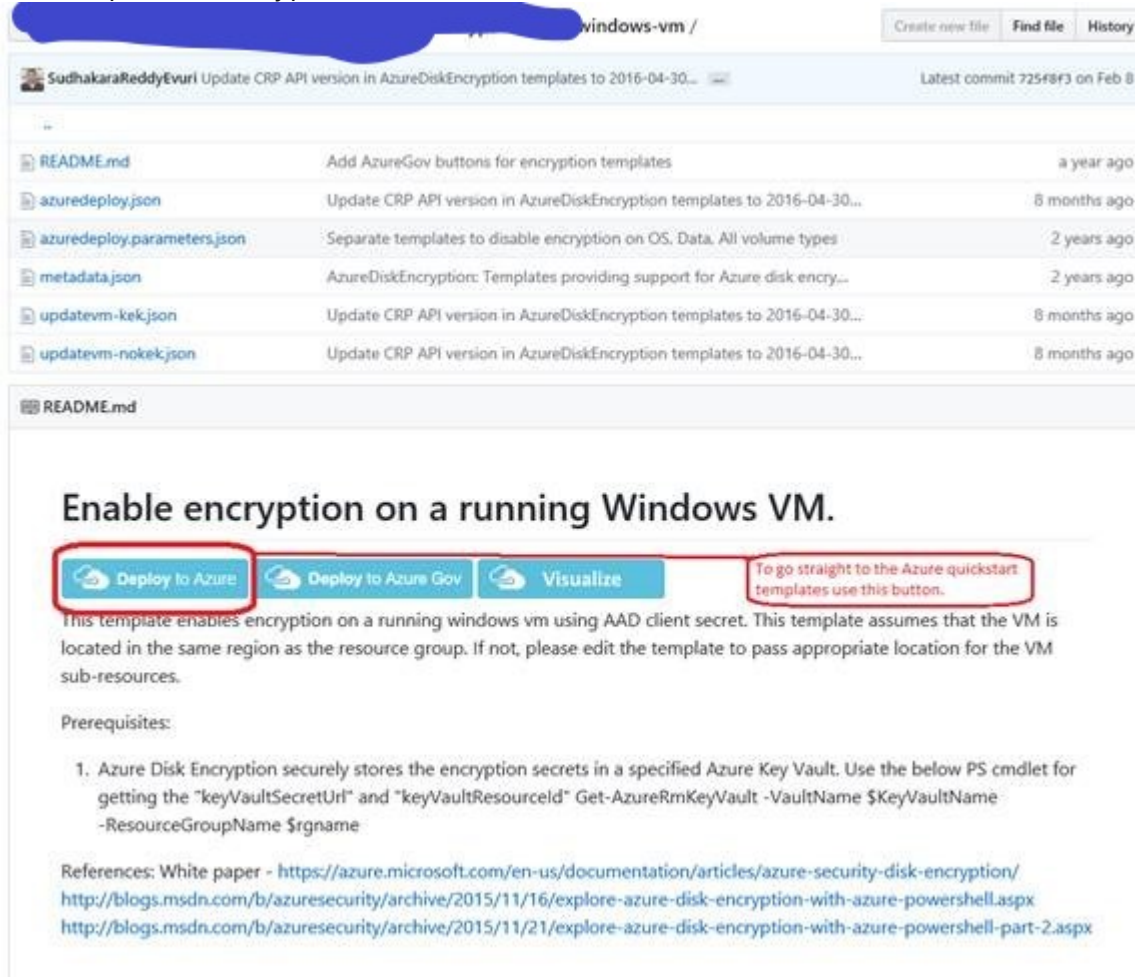
```
Get-AzVmDiskEncryptionStatus -ResourceGroupName $RGName -VMName $VMName
```

6. You should be able to see that both the OS volume and the data volumes are now encrypted:

```
OsVolumeEncrypted      : Encrypted
DataVolumesEncrypted   : Encrypted
OsVolumeEncryptionSettings : Microsoft.Azure.Management.Compute.Models.DiskEncryptionSettings
ProgressMessage         : OsVolume: Encrypted, DataVolumes: Encrypted
```

Process to encrypt VM with KEK- Template

1. The template to encrypt a VM with KEK is [here](#) .



Repository: windows-vm /

Create new file Find file History

SudhakarReddyEvuri Update CRP API version in AzureDiskEncryption templates to 2016-04-30... Latest commit 725f8f3 on Feb 8

File	Description	Time
README.md	Add AzureGov buttons for encryption templates	a year ago
azuredeploy.json	Update CRP API version in AzureDiskEncryption templates to 2016-04-30...	8 months ago
azuredeploy.parameters.json	Separate templates to disable encryption on OS, Data, All volume types	2 years ago
metadata.json	AzureDiskEncryption: Templates providing support for Azure disk encry...	2 years ago
updatevm-kek.json	Update CRP API version in AzureDiskEncryption templates to 2016-04-30...	8 months ago
updatevm-nokek.json	Update CRP API version in AzureDiskEncryption templates to 2016-04-30...	8 months ago

README.md

Enable encryption on a running Windows VM.

[Deploy to Azure](#) [Deploy to Azure Gov](#) [Visualize](#)

To go straight to the Azure quickstart templates use this button.

This template enables encryption on a running windows vm using AAD client secret. This template assumes that the VM is located in the same region as the resource group. If not, please edit the template to pass appropriate location for the VM sub-resources.

Prerequisites:

1. Azure Disk Encryption securely stores the encryption secrets in a specified Azure Key Vault. Use the below PS cmdlet for getting the "keyVaultSecretUri" and "keyVaultResourceId" Get-AzureRmKeyVault -VaultName \$KeyVaultName -ResourceGroupName \$rgname

References: White paper - <https://azure.microsoft.com/en-us/documentation/articles/azure-security-disk-encryption/>
<http://blogs.msdn.com/b/azuresecurity/archive/2015/11/16/explore-azure-disk-encryption-with-azure-powershell.aspx>
<http://blogs.msdn.com/b/azuresecurity/archive/2015/11/21/explore-azure-disk-encryption-with-azure-powershell-part-2.aspx>

2. Once you are on the Azure quickstart template, fill in the required fields. You can then save the template so that you can reuse when needed.

Home > Enable encryption on a running Windows VM.

Enable encryption on a running Windows VM.

Azure quickstart template

TEMPLATE

201-encrypt-running-windows-vm
2 resources

Edit template Edit parameters Learn more

BASICS

* Subscription: Microsoft Azure Internal Consumption

* Resource group: ☒ Create new ☐ Use existing
Create a resource group

* Location: East US

SETTINGS

* Vm Name

* Aad Client ID

* Aad Client Secret

* Key Vault Name

* Key Vault Resource Group

Use Existing Kek: nokek

Key Encryption Key URL

Volume Type: All, Data or OS: All

Sequence Version: 1.0

TERMS AND CONDITIONS

Template information Azure Marketplace Terms Azure Marketplace

By clicking "Purchase," I (a) agree to the applicable legal terms associated with the offering; (b) authorize Microsoft to charge or bill my current payment method for the fees associated the offering(s), including applicable taxes, with the same billing frequency as my Azure subscription, until I discontinue use of the offering(s); and (c) agree that, if the deployment involves 3rd party offerings, Microsoft may share my contact information and other details of such deployment with the publisher of that offering.

☐ I agree to the terms and conditions stated above

Only required for KEK (wrapped BEK) encryption.

3. Press the Purchase button to run the template.

Get a list of all encrypted VMs in your subscription

1. If you have multiple VMs in your subscription and you want to list the OS volume and data volumes encryption status for all VMs to see which of the VMs are encrypted, the below cmdlets show you how to do that.

```
$osVolEncrypted = {(Get-AzVMDiskEncryptionStatus -ResourceGroupName $_.ResourceGroupName -VMName $_.Name)
$dataVolEncrypted= {(Get-AzVMDiskEncryptionStatus -ResourceGroupName $_.ResourceGroupName -VMName $_.Name)
Get-AzVm | Format-Table @{Label="MachineName"; Expression={$_.Name}}, @{Label="OsVolumeEncrypted"; Ex
```

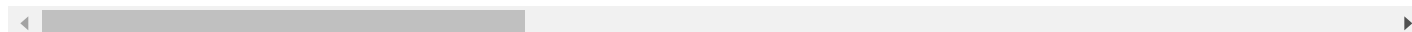
2. Here is one way you can see the list of VMs that are encrypted in a structured output:

MachineName	OsVolumeEncrypted	DataVolumesEncrypted
TestVM1	Unknown	Unknown
TestVM2	Encrypted	NotEncrypted
TestVM3		
TestVM4	Encrypted	Encrypted
TestVM5	NotEncrypted	NotEncrypted
TestVM6	...tionInProgress	EncryptionInProgress

Get a list of all disk encryption secrets used for encrypting VM in your subscription

1. The Azure Disk Encryption functionality uploads encryption secrets corresponding to all the volumes into the Key Vault specified while enabling encryption. If you would like to see all the disk encryption secrets in a given Key Vault written by Azure Disk Encryption and the corresponding machine names and volume letters, the following syntax will provide that report for you:

```
Get-AzKeyVaultSecret -VaultName $KeyVaultName | where {$_.Tags.ContainsKey('DiskEncryptionKeyFileName
```



2. It will be structured and displayed in similar format:

MachineName	Volume	EncryptionKeyURL
MYSECUREVM	D:	https://mysecurevault.vault.azure.net:443/secrets/7832CE5C-A252-4E50-B3CC-2A163
MYSECUREVM	C:	https://mysecurevault.vault.azure.net:443/secrets/FA44FF92-91F0-4312-A1E8-224B7



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 <input type="checkbox"/> 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>