

# Wrong Encryption Status Shown on the Portal\_Encryption

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

## Tags

cw.Azure-Encryption

cw.TSG

## Contents


- [Symptoms](#)
- [Root Cause](#)
- [Mitigation](#)
- [Need additional help or have feedback?](#)

## Symptoms

Encryption status in Azure Portal is not reflecting correct.

## Root Cause

There can be multiple causes why the Encryption Status is not accurate in Azure Portal.

Cause 1. A fix is expected to be released in March. Check status here [https://msazure.visualstudio.com/One/\\_workitems/edit/5607713](https://msazure.visualstudio.com/One/_workitems/edit/5607713) 

Cause 2. Encryption inside guest OS should kick in automatically but in order to reflect in Azure Portal the encryption status for the new disk a Stop (de-allocate) must be performed in order for the extension to communicate the new status to the host.

Cause 3. This occurs when you disable encryption from OS level directly. The extension will not be updated by the OS if you manipulate manually Bitlocker as OS level. The manipulation of encryption must be done always using the high level commands for ADE extension.

## Mitigation

### Cause 1

A fix is expected to be released in March. Check status here [https://msazure.visualstudio.com/One/\\_workitems/edit/5607713](https://msazure.visualstudio.com/One/_workitems/edit/5607713)

### Cause 2

Encryption inside guest OS should kick in automatically but in order to reflect in Azure Portal the encryption status for the new disk a Stop (de-allocate) must be performed in order for the extension to communicate the new status to the host.

### Cause 3

This occurs when you disable encryption from OS level directly. Cause: The extension will not be updated by the OS if you manipulate manually Bitlocker as OS level. The manipulation of encryption must be done always using the high level commands for ADE extension.

In this case there are 2 options

- Create new VM using the fixed disk
- Swap OS disk - most common (this is supported for single pass method - without AAD).


For both option you need to re-run encryption using Set-AzVMDiskEncryptionExtension cmdlet.

Example:

```
Set-AzVMDiskEncryptionExtension -ResourceGroupName $RGName -VMName $VMName -DiskEncryptionKeyVaultUrl $DiskEnc
```



## 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 <a href="#">Azure Encryption SMEs</a>  for faster assistance.</p> <p>Make sure to use the <a href="#">Ava process</a> for faster assistance.</p>	<p>Use the <a href="#">Azure Encryption Feedback</a> form to submit detailed feedback on improvements or new content ideas for Azure Encryption.</p> <p><b>Please note</b> 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 <a href="#">Azure Encryption Kudos</a> form to submit kudos on the page. Kudos will help us improve our wiki content overall!</p> <p><b>Please note</b> the link to the page is required when submitting kudos!</p>