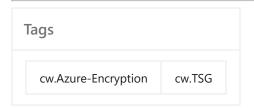
# ProtectKeyWithExternalKey Failed with 2150695023\_Encryption

Last updated by | Clayton Fuselier | Apr 14, 2022 at 9:46 AM PDT



#### **Contents**

- Symptom
- Mitigation
- Resolution
- Need additional help or have feedback?

### **Symptom**

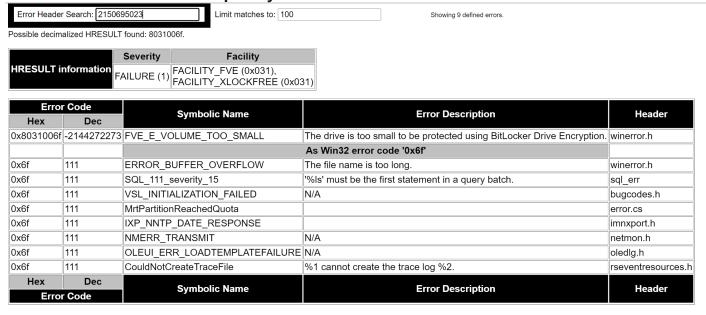
1. When the customer tries to enable ADE, he will get the following outcome on powershell

```
Failed to configure bitlocker as expected. Exception: ProtectKeyWithExternalKey failed with 215069502 InnerException: , stack trace: at Microsoft.Cis.Security.BitLocker.BitlockerIaasVMExtension.BitlockerWmi.Win32EncryptableVolumeWrap. at Microsoft.Cis.Security.BitLocker.BitlockerIaasVMExtension.BitlockerExtension.GenerateProtectorForV at Microsoft.Cis.Security.BitLocker.BitlockerIaasVMExtension.BitlockerExtension.GenerateAndUploadProt at Microsoft.Cis.Security.BitLocker.BitlockerIaasVMExtension.BitlockerExtension.EnableEncryption() in at Microsoft.Cis.Security.BitLocker.BitlockerIaasVMExtension.BitlockerExtension.HandleEncryptionOpera at Microsoft.Cis.Security.BitLocker.BitlockerIaasVMExtension.BitlockerExtension.OnEnable() in C:\\_w
```

## Mitigation

- 1. First review the Errors Online with the ID (in this case the iD is 2150695023) to double check it:
- Error lookup ☑

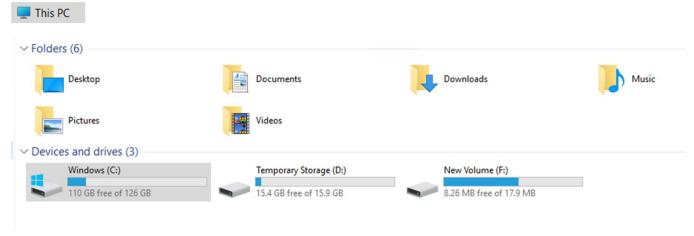
#### Note: To access the error lookup link you should be connected to the VPN



2. After confiming that the error is realted to "The drive is too small to be protected using Bitlocker Drive Encryption".

Request the following information:

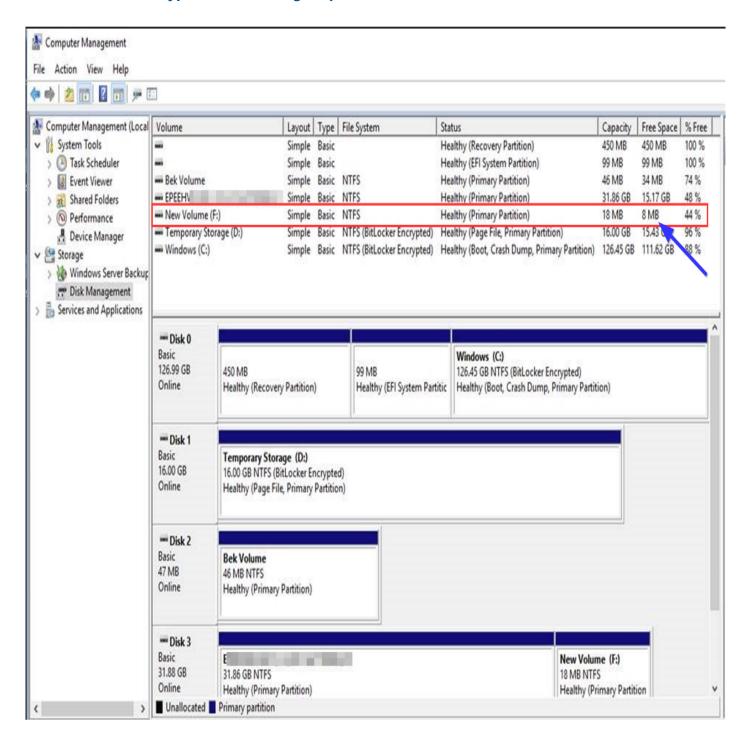
- Request to deallocate the VM and start it again in order to confirm if after that the encryption status is updated in the VM disks and in the portal.
- Request an output of the result when you execute in CMD manage-bde -status (add it as an attachment and uploaded due to length of the output)
- Request a screenshot of the disks when you access the files explorer and go to my PC or This PC (like the example below):



Request an output of the disk management.

#### Resolution

Once the information is provided, and if after the restart the encryption status is not being updated in the portal and inside the VM, review the size of the disks and confirm if the F: drive or other have more than 250MB free to be used (like in the example image). (ignore the Bek Volume and the EFI System Partition)



Ask the customer to set the drive with less than 250MB of free space to "offline". Then retry the encryption process. Usually an error can appear during the encryption process, however ask the customer to deallocate the VM and start it again in order to confirm if the status is updated and marked as encrypted.

Note: In other cases the customer decided to delete the problematic partition (F: in this example), and that fix the issue. However that decision should be analyzed by the customer after confirm that the partition is not being use by them.

## Need additional help or have feedback?

To engage the Azure Encryption SMEs	To provide feedback on this page	To provide kudos on this page
Please reach out to the Azure Encryption  SMEs of for faster assistance.  Make sure to use the Ava process for faster assistance.	Use the Azure Encryption Feedback form to submit detailed feedback on improvements or new content ideas for Azure Encryption.  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.	Use the Azure Encryption  Kudos form to submit kudos on the page. Kudos will help us improve our wiki content overall!  Please note the link to the page is required when submitting kudos!