

# ADE with ASR\_Encryption

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

## Tags

cw.Azure-Encryption

cw.How-To

## Contents

- [Summary](#)
- [Reference](#)
- [Instructions](#)
  - [ASR on Failover VMs](#)
  - [Gather Logs](#)
  - [Escalate to ADE Teams Channel](#)
- [Need additional help or have feedback?](#)


## Summary

There are two scenarios where you are going to apply this article:

- When customer is reporting a mismatch in encryption status after failover using ASR.
- When customer is asking how to set up ASR with Dual pass ADE.

**This How To TSG does not explain how to set up ADE with ASR. If the customer wants to set up ASR please refer to the link in the "References" section.**

## Reference

- <https://docs.microsoft.com/en-us/azure/site-recovery/azure-to-azure-how-to-enable-replication-ade-vm>  


## Instructions

### ASR and Encryption Method

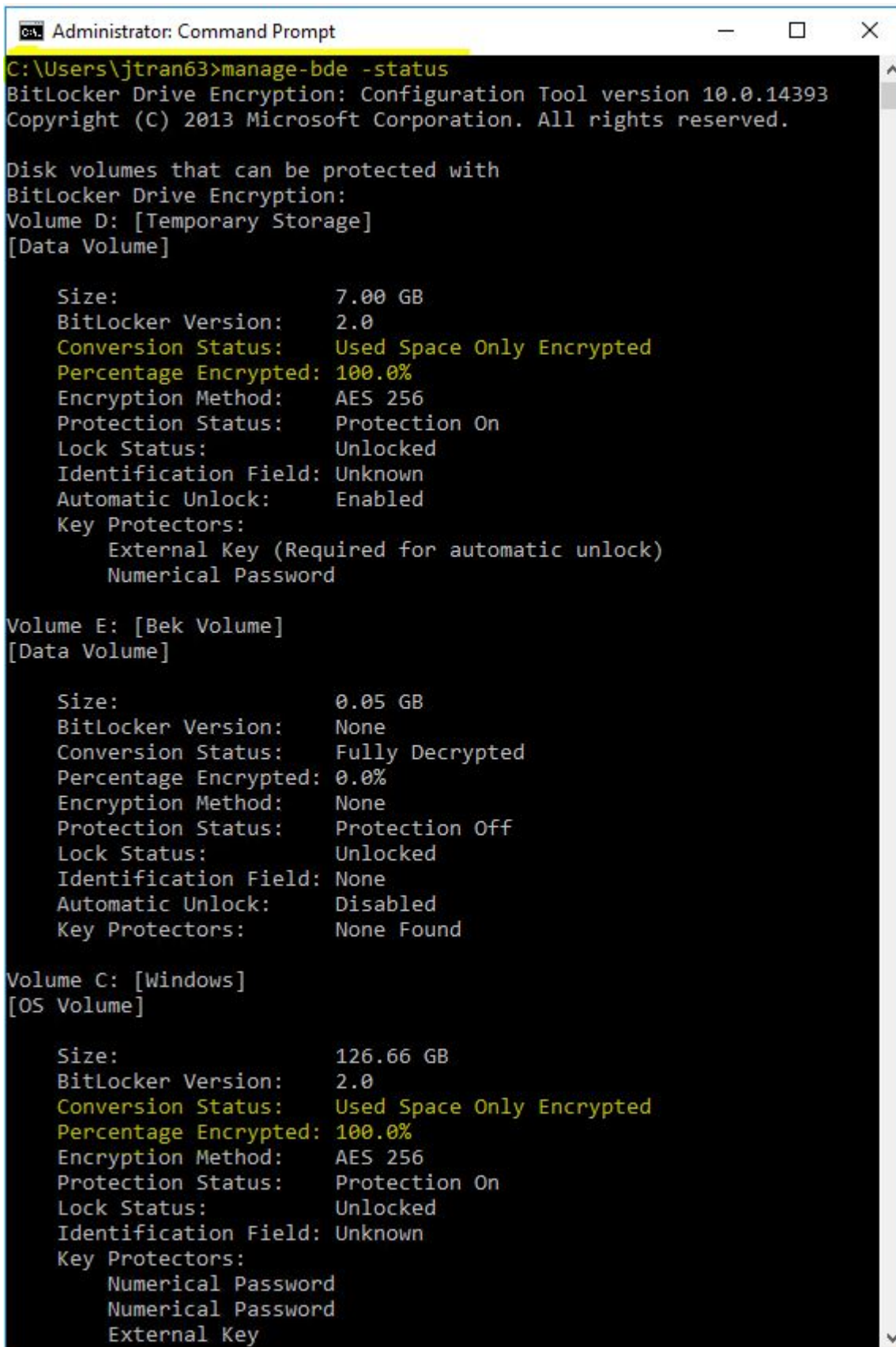
1. If customer is asking how to set up ASR with ADE please refer to the link under "References"
  - Note: If customer VM is currently encrypted, find the extension version within ASC and encryption method used.
2. Extension version 1.1 (with AAD) is supported for ASR. Extension version 2.2 (without AAD) is now supported as well.

### ASR on Failover VMs

Once the customer has verified that failover occurred from one (primary) region to another using ASR, the failover VM might show a mismatch in encryption status within the portal, PS, or CLI.

1. Confirm encryption status of the VM internally.

- RDP into VM -> Open CMD prompt -> Run "manage-bde -status"
  - If the VM shows 100%, fully encrypted. Proceed to next step.
  - If the VM shows 0%, fully decrypted. Proceed to confirm ASR replication steps using the link in the "Reference" section to ensure customer replicated encrypted VMs correctly.



```
Administrator: Command Prompt
C:\Users\jtran63>manage-bde -status
BitLocker Drive Encryption: Configuration Tool version 10.0.14393
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

Disk volumes that can be protected with
BitLocker Drive Encryption:
Volume D: [Temporary Storage]
[Data Volume]

    Size:                7.00 GB
    BitLocker Version:    2.0
    Conversion Status:    Used Space Only Encrypted
    Percentage Encrypted: 100.0%
    Encryption Method:    AES 256
    Protection Status:    Protection On
    Lock Status:          Unlocked
    Identification Field: Unknown
    Automatic Unlock:     Enabled
    Key Protectors:
        External Key (Required for automatic unlock)
        Numerical Password

Volume E: [Bek Volume]
[Data Volume]

    Size:                0.05 GB
    BitLocker Version:    None
    Conversion Status:    Fully Decrypted
    Percentage Encrypted: 0.0%
    Encryption Method:    None
    Protection Status:    Protection Off
    Lock Status:          Unlocked
    Identification Field: None
    Automatic Unlock:     Disabled
    Key Protectors:       None Found

Volume C: [Windows]
[OS Volume]

    Size:                126.66 GB
    BitLocker Version:    2.0
    Conversion Status:    Used Space Only Encrypted
    Percentage Encrypted: 100.0%
    Encryption Method:    AES 256
    Protection Status:    Protection On
    Lock Status:          Unlocked
    Identification Field: Unknown
    Key Protectors:
        Numerical Password
        Numerical Password
        External Key
```

# 1. Confirm extension installed on Failover VM

## o Within ASC -> Extensions Tab:

- If extension is already installed and there is still a mismatch in encryption status proceed to "Gather Logs" section.
- If extension is not installed advise the customer to install extension.

- With AAD: <https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-windows-aad#enable-encryption-on-a-newly-added-data-disk> ☑
  - Without AAD: <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-windows#enable-encryption-on-a-newly-added-data-disk> ☑
  - Once extension is installed. Confirm encryption status within the Portal, on PS, and internally (manage-bde).
- If the encryption status is still showing as a mismatch, proceed to "Gather Logs".
  - **Note: A mismatch is where the encryption status shows enabled in one location and disabled in another. i.e manage-bde -status vs. Portal status.**

## Gather Logs

1. Once logs and screenshots are gathered, proceed to next section.
  - C:\WindowsAzure\Logs\Plugins\Microsoft.Azure.Security.AzureDiskEncryption
  - C:\Packages\Plugins\Microsoft.Azure.Security.AzureDiskEncryption\RuntimeSettings
  - C:\Windows\System32\winevt\Logs\Microsoft-Windows-BitLocker%4BitLocker Management.evtx
  - C:\Windows\System32\winevt\Logs\Microsoft-Windows-BitLocker-DrivePreparationTool%4Operational.evtx
  - Output of "manage-bde -status"

## Escalate to ADE Teams Channel

## 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 <b>Azure Encryption SMEs</b> ☑ for faster assistance.</p> <p>Make sure to use the <b>Ava process</b> for faster assistance.</p>	<p>Use the <b>Azure Encryption Feedback</b> 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 <b>Azure Encryption Kudos</b> 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>