ProtectKeyWithExternalKey Failed with 2150695006_Encryption

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

Tags

cw.Azure-Encryption cw.TSG

Contents

- Symptom
- Mitigation

- Need additional help or have feedback?

Symptom

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

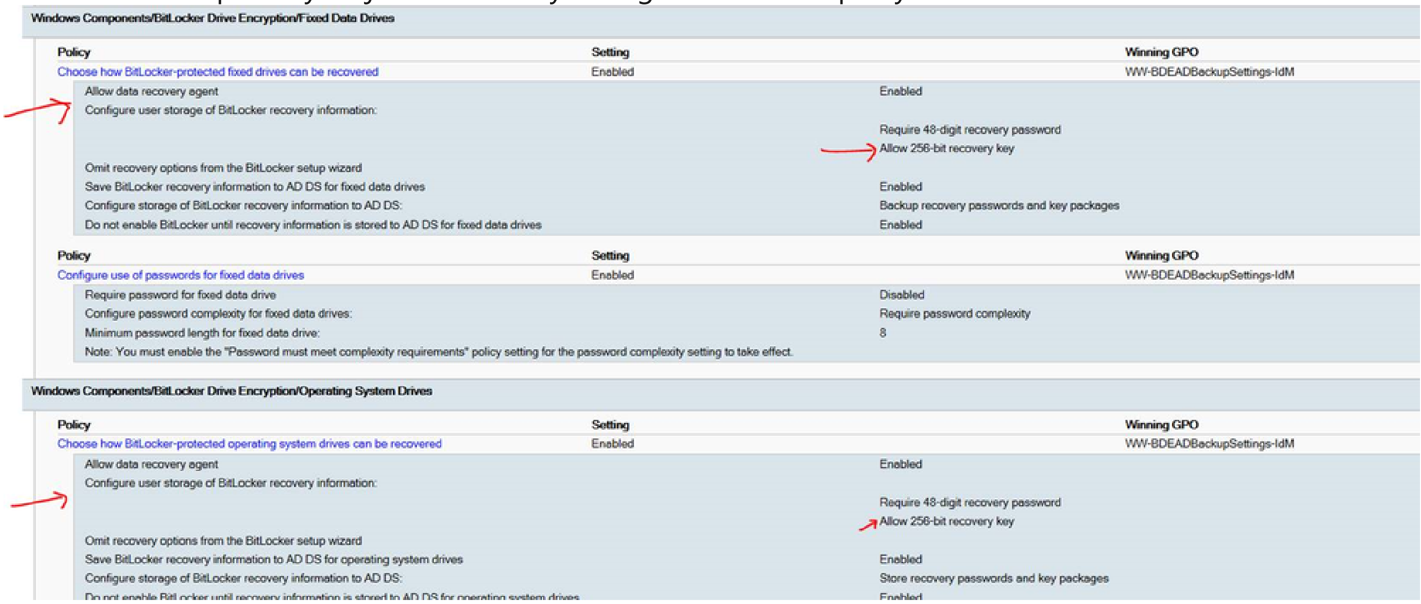
```
Set-AzureRmVMDiskEncryptionExtension : Long running operation failed with status 'Failed'. ErrorCode:

InnerException: , stack trace:    at Microsoft.Cis.Security.BitLocker.BitlockerIaasVMExtension.Bitloc

   at Microsoft.Cis.Security.BitLocker.BitlockerIaasVMExtension.BitlockerOperations.GenerateKeyForVol
   at Microsoft.Cis.Security.BitLocker.BitlockerIaasVMExtension.BitlockerExtension.GenerateAndUploadP
   at Microsoft.Cis.Security.BitLocker.BitlockerIaasVMExtension.BitlockerExtension.GenerateAndUploadO
   at Microsoft.Cis.Security.BitLocker.BitlockerIaasVMExtension.BitlockerExtension.EnableEncryption()
   at Microsoft.Cis.Security.BitLocker.BitlockerIaasVMExtension.BitlockerExtension.HandleEncryptionOp
   at Microsoft.Cis.Security.BitLocker.BitlockerIaasVMExtension.BitlockerExtension.OnEnable()'.
```

Mitigation

1. Ensure the Group Policy Object is correctly configured to backup keys in ADDS.



Windows Components/BitLocker Drive Encryption/Fixed Data Drives

Policy	Setting	Winning GPO
Choose how BitLocker-protected fixed drives can be recovered	Enabled	WW-BDEADBackupSettings-IdM

Allow data recovery agent	Enabled
Configure user storage of BitLocker recovery information:	
	Require 48-digit recovery password
	Allow 256-bit recovery key
Omit recovery options from the BitLocker setup wizard	
Save BitLocker recovery information to AD DS for fixed data drives	Enabled
Configure storage of BitLocker recovery information to AD DS:	Backup recovery passwords and key packages
Do not enable BitLocker until recovery information is stored to AD DS for fixed data drives	Enabled

Policy	Setting	Winning GPO
Configure use of passwords for fixed data drives	Enabled	WW-BDEADBackupSettings-IdM

Require password for fixed data drive	Disabled
Configure password complexity for fixed data drives:	Require password complexity
Minimum password length for fixed data drive:	8

Note: You must enable the "Password must meet complexity requirements" policy setting for the password complexity setting to take effect.

Windows Components/BitLocker Drive Encryption/Operating System Drives

Policy	Setting	Winning GPO
Choose how BitLocker-protected operating system drives can be recovered	Enabled	WW-BDEADBackupSettings-IdM

Allow data recovery agent	Enabled
Configure user storage of BitLocker recovery information:	
	Require 48-digit recovery password
	Allow 256-bit recovery key
Omit recovery options from the BitLocker setup wizard	
Save BitLocker recovery information to AD DS for operating system drives	Enabled
Configure storage of BitLocker recovery information to AD DS:	Store recovery passwords and key packages
Do not enable BitLocker until recovery information is stored to AD DS for operating system drives	Enabled

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** 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!